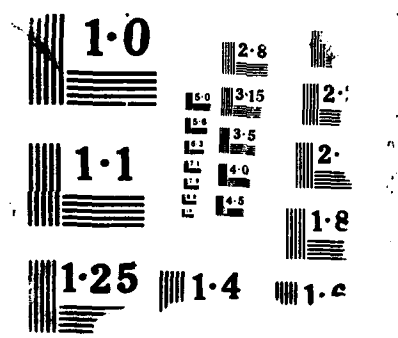
AD-A195 444   THE PROPOSED NAVAL POSTGRADUATE SCHOOL CAMPUS NETWORK: 1/2
COMPUTER COMMUNICATIONS FOR THE 1990'S(U) NAVAL
POSTGRADUATE SCHOOL MONTEREY CA K M LEAHY MAR 88

UNCLASSIFIED   F/G 12/7   NL


1·0
2·8
3·15
5·0
3·5
1·1
4·0
4·5
1·8
1·25
1·4

(2)

AD-A195 444

NAVAL POSTGRADUATE SCHOOL
Monterey, California

DTIC FILE COPY

DTIC
S ELECTE D
JUL 0 8 1988
D

THESIS

THE PROPOSED NAVAL POSTGRADUATE SCHOOL CAMPUS NETWORK: COMPUTER COMMUNICATIONS FOR THE 1990's

by

Kevin M. Leahy

March 1988

Thesis Advisor: Norman Schneidewind

Approved for public release; distribution is unlimited

4

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; Distribution is unlimited
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b. OFFICE SYMBOL (If applicable) Code 54	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000		7b. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
8a. NAME OF FUNDING / SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State, and ZIP Code)

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
THE PROPOSED NAVAL POSTGRADUATE SCHOOL CAMPUS NETWORK: COMPUTER COMMUNICATIONS FOR THE 1990's (u)

12. PERSONAL AUTHOR(S)
Leahy, Kevin M.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Master's Thesis	FROM ______ TO ______	1988 March	107

16. SUPPLEMENTARY NOTATION
"The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government."

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Metropolitan network; Fiber optics; Local area network

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

Computer data communication at the Naval Postgraduate School is about to be revolutionized. No longer will departmental computer users be limited to the resources available to them at their site. The NPS Connectivity and Networking Committee has proposed an innovative, high-speed Campus Network which promises to provide connectivity to virtually all NPS computing resources, regardless of building location or controlling department.

This paper describes the composition of the Connectivity and Networking Committee and explains the network proposal that its members made. Certain aspects of this proposal are elaborated upon, including fiber optics as a transmission medium and the Committee's recommendations for inter-networking protocols.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code)	22c. OFFICE SYMBOL
Schneidewind, Norman	(408) 646-2768	Code 54Ss

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

Approved for public release; distribution unlimited

The Proposed Naval Postgraduate School Campus Network: Computer Communications for the 1990's

by

Kevin M. Leahy
Captain, United States Marine Corps
B.A., Saint Joseph's University, 1977
M.B.A., National University, 1986

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1988

Author: Kevin M Leahy
Kevin M. Leahy

Approved by: N. F. Schneidewind
N. F. Schneidewind, Thesis Advisor

Y. K. Mortagy
Y. K. Mortagy, Second Reader

David R. Whipple, Chairman
Department of Administrative Sciences

James M. Fremgen,
Acting Dean of Information and Policy Sciences

ABSTRACT

Computer data communication at the Naval Postgraduate School is about to be revolutionized. No longer will departmental computer users be limited to the resources available to them at their site. The NPS Connectivity and Networking Committee has proposed an innovative, high-speed Campus Network which promises to provide connectivity to virtually all NPS computing resources, regardless of building location or controlling department.

This paper describes the composition of the Connectivity and Networking Committee and explains the network proposal that its members made. Certain aspects of this proposal are elaborated upon, including fiber optics as a transmission medium and the Committee's recommendations for inter-networking protocols.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

A. BACKGROUND

In November, 1987, a proposal was forwarded to the NPS Mainframe Computer Replacement Committee which called for the installation of a high-speed campus backbone network to support the instructional, research and administrative requirements at the school through the decade of the 1990's.

This innovative recommendation was contained in the final report of the NPS Connectivity and Network Committee. The Committee consisted of fourteen members representing instructors, researchers, students, staff officers and tenant users of the NPS mainframe computer.

The group had as its charter to investigate the feasibility of a campus-wide backbone network connecting the various departmental local area networks (LAN's), and to make recommendations on the design of such a system. Activation of the campus backbone network would allow the user to chose the most appropriate device for his application. This, in turn, is expected to lead to greater efficiency in the use of the School's computing resources.

The Committee's approach was to analyze both the networking needs of the NPS community, and to examine the current and projected state of the art in networking technology. After two months of research and preparation,

the Committee members reached agreement on the final report. That document, as presented to the full NPS Mainframe Computer Replacement Committee provides the basis of this paper.

B. PURPOSE

The purpose of this paper is to elaborate upon the work done by the Connectivity and Network Committee, and to add detail to certain technical and managerial facets of the proposed campus network.

The target audience of the report are the future users and network administrators interested in the idea of high speed data communication at NPS. Although this report does not dwell on the technicalities of data networking, it presumes that the reader has had some exposure to the fundamentals of computer communications and local area networking.

C. ORGANIZATION OF STUDY

Each of the following chapters deals with a separate aspect of the proposed NPS Campus Network. The topics are:

1. The Campus Network Proposal

A discussion of the Connectivity and Networking Committee proposal is contained in Chapter II. Included are the origins, composition and workings of the Committee, as well as an explanation of the network proposal as envisioned by the Committee members.

b. <u>The Navy's Base Information Transfer System</u>

In Chapter III an on-going Navy Base networking program called the Base Information Transfer System is described. Since the program will influence Navy shore communications in the 1990's, this paper examines how it will affect the NPS Campus Network.

c. <u>Fiber Optics in Communications</u>

Chapter IV addresses the emerging fiber optics technologies and the way that the Fiber Distributed Data Interface will influence high-speed data communications including networks such as the NPS Campus Network.

d. <u>Internetworking</u>

The leading methods used to allow varied vendor's products to communicate across large network are discussed in Chapter V. This is a critical issue to managers of networks like the one proposed for NPS since the entire matter of communications protocols is currently in a marked state of flux.

II. THE CONNECTIVITY AND NETWORKING SUBCOMMITTEE (CNS)

The Report of the Connectivity and Networking Subcommittee contained a proposal for an NPS Campus Area Network connecting departmental networks throughout the University. This proposal, when adopted and implemented, will revolutionize the computing environment at the Naval Postgraduate School.

This chapter will study the origin of the Subcommittee, follow its progress as it developed the network proposal, and finally, explain the visionary network which was recommended in its final report.

A. ORIGIN OF THE SUBCOMMITTEE

It was mid-1987, and time to plan for the replacement of the NPS Computer Center's aging IBM 3033 Mainframe Computer. A Mainframe Computer Replacement Committee was created to study the matter and advise the Computer Center staff on most effective way to maintain high-quality computer service to the NPS environment in the post-IBM 3033 era.

The funding for this replacement project, which had already been budgeted, was based on the costs a new mainframe computer. But rather than simply shopping for a new mainframe, the Replacement Committee chose to consider a number of options, recognizing that many alternatives to

large scale centralized computing had emerged since the replacement project was first envisioned.

1. Alternatives to Mainframe Computing

Various computing options were available to faculty and students at NPS, and the Replacement Committee was interested in providing the most computing service with the funds provided. Therefore a number of computing options were investigated.

Using high speed **supercomputers** for specialized computational tasks was one partial alternative, or complement, to a general-purpose mainframe. This appealed to a large segment of the NPS user community, particularly those involved in mathematical and scientific research.

Another reality at NPS was the proliferation of dedicated **graphics and engineering workstations.** These workstations provided specialized computing abilities which are not easily replicated on mainframe terminals.

The rapid emergence of **end user computing** (EUC), and the celebrated shift toward microcomputers was yet another factor that the Replacement Committee members considered. Closely related to EUC was the growth of departmental micro-computer based **local area networks** (LAN's). These LAN's are economical ways for individual departments to provide their faculty and students with many of the services (wordprocessing, database and spreadsheet applications, and

print service) which previously had only been available through the mainframe or not available at all.

As the result of these increased options, the Committee decided to form three subcommittees to study these possibilities in more depth. Specifically, these subcommittees were to investigate whether NPS computer users would be better served by using portions of the resources allocated for mainframe replacement on some of the alternatives listed above. Figure 2.1 illustrates the relationship of the Mainframe Replacement Committee with its various subcommittees and working groups.

One subcommittee looked into the possibility of creating an NPS supercomputing facility with a portion of the replacement funds. This facility was to be designed to meet the growing requirement for very high speed numerical and scientific calculations. Another subcommittee investigated the best way to provide computerized library services to the Knox Library users and staff.

The third subcommittee formed by the Mainframe Replacement Committee was the **Connectivity and Network Subcommittee**. The CNS was asked to provide recommendations on the installation of a high-speed campus backbone network to allow data communication among the numerous departmental LAN's.

The work of the CNS, which culminated in its November, 1987 publication of "Connectivity and Network

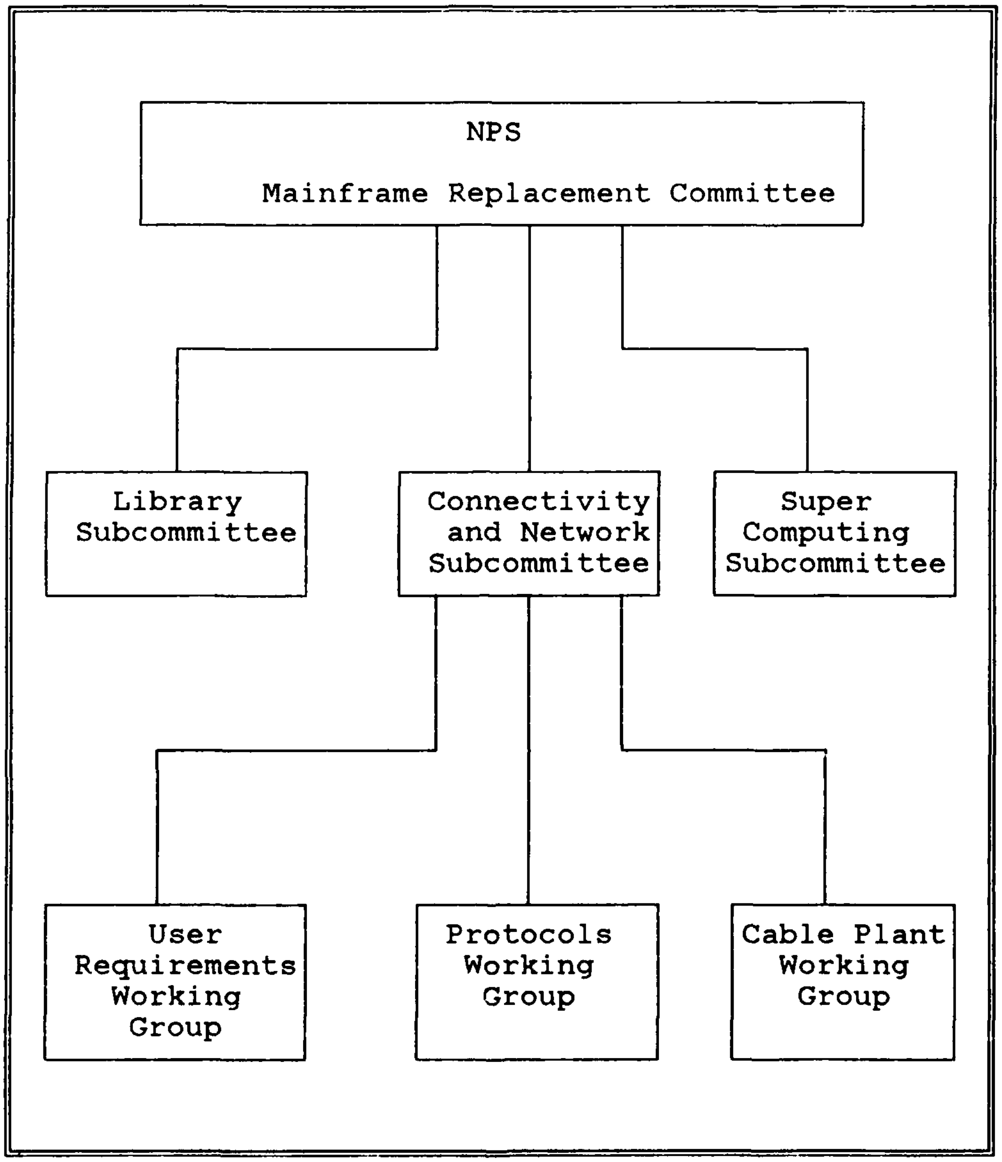


Figure 2.1 Structure of the NPS Mainframe Replacement Committee and Subordinate Committees

Report, Campus Computer Network," [Ref. 1], provides the foundation for this thesis.

B. COMPOSITION OF THE CNS

The CNS consisted of 14 members representing various segments of the NPS community. Spokesmen from the assorted Engineering and Science departments were present, as were representatives from tenant activities, curricular offices and support organizations. Researchers, instructors, students and administrators were all spoken for.

1. Working Group Approach

Although the CNS members met weekly as a group, the work accomplished during each of these meetings was only a portion of the Subcommittee's output.

Individually, and in working groups, CNS members researched issues assigned to them and contributed their findings to the full body. Three working groups were created to study each of the following aspects of the campus network:

- The network cable plant;
- The network protocols;
- The network user requirements, in three areas:
  a. research;
  b. instruction; and
  c. administrative support.

The output of each of the three working groups was incorporated into the CNS final report.

C. PURPOSE

At its second meeting, the group decided on the purpose of the proposed campus network:

> The purpose of the Campus Area Network is to provide for the instructional, research and administrative support services to the NPS community through the 1990's. (Ref. 2: p. 1)

With this framework in mind, the CNS members set out to develop a viable proposal for such a network.

D. WORKINGS OF THE CNS

The CNS held its first meeting on September 11, 1987, and conducted seven weekly sessions before forwarding its recommendation in November. The minutes of each meeting were compiled and distributed electronically. Members used electronic messaging via the NPS mainframe and the DDN to correspond between meetings.

Discussion at the meetings was free-wheeling, and often spirited, owing largely to the varied background which each member brought to the group. Numerous networking approaches were suggested and examined, as were different network service strategies. Although the Subcommittee's findings were not always unanimous, they do represent the conclusions of a large majority of the participants.

E. THE ISSUES

Figure 2.2 lists the topics which became the subject of the greatest discussion by the CNS. Each of the issues will be briefly covered in this section.

1. Cable Plant

The Subcommittee members knew that the campus network cabling represented the most labor-intensive and therefore the most expensive portion of the project. For that reason it was decided early on that the cabling plan be devised with relative permanence in mind. "Any cable which is laid in conjunction with this project must meet the network's needs for the next 20 years." [Ref. 3: p. 1]

The Subcommittee considered the installation of **coaxial cable**, but its bulk and limited bandwidth were serious limitations. There are actually places on campus where there is no more room in the wiring trenches to insert any more coaxial cable. And coaxial cable, with its susceptibility to interference and signal attenuation, is not the favored medium for very high speed networks. For these reasons, the CNS members chose to use fiber optic cable on the campus network. Chapter Four of this report discusses the advantages of the fiber optic medium in more detail.

2. Network Access Method

Network access is concerned with the control method to be used in entering the network. The two prospective

CNS Discussion Issues
- Cable Plant Life Expectancy - Network Access Method - Inclusion of Administrative Services - Network Management - Assured Internetworking - Geographical Coverage - Funding

Figure 2.2 CNS Discussion Issues

choices were the CSMA/CD (Carrier Sense, Multiple-Access with Collision Detection) approach, and the token-passing method. Discussion of these two control methods is not included here. Readers interested in further discussion of network access are directed to [Ref. 4].

Proponents of a **CSMA/CD** network pointed out that this approach was a more mature technology; the one used by most contemporary LAN vendors. One CSMA/CD network approach is prescribed in the Institute of Electrical and Electronics Engineers IEEE 802.3 standard. And CSMA/CD is generally cheaper to implement on lower speed networks. Many examples of campus networks were installed using this contention-access method.

On the other hand, a managed access network similar, but on a larger scale, to the **token-passing** arrangement described in (IEEE) Standard 802.5, would provide greater throughput at higher data loads. Although token-passing techniques were not as widely used as CSMA/CD, it was a managed access method which American National Standards Institute (ANSI) had adopted for its high speed Fiber Distributed Data Interface (FDDI) standard, which was to be published in the near future.

The two access methods were presented to the CNS in the form of "straw man" proposals, to allow each member to gain a better understanding of the issues. The CNS members were presented with two straw man campus networks each

representing one of the contending access methods. During its 9 October meeting, the Subcommittee approved the plan for "...a high capacity fiber optics based backbone ring using managed access via token-passing." [Ref. 5: p. 1]

3. Inclusion of Administrative Services

During the early meetings it was unclear whether the inclusion of administrative data was within the charter of the Subcommittee, or if the network was to be used exclusively for research and instructional purposes. Examples of these administrative data are Public Works work orders, requests for status from the Supply or Comptroller Departments, reconciliation of travel claims and the hundreds of similar support documents which are used at NPS on a daily basis.

The CNS decided that the campus network should include administrative traffic [Ref. 2: p. 1]. The CNS concluded that to establish separate networks for different types of information would be an inefficient use of resources, and very confusing to users.

4. Network Management

It is one thing to install a large facility like the NPS Campus Network, and quite another to manage and maintain it! Operational funding, manpower, traffic prioritization, maintenance and security are just a few of the managerial issues which the CNS examined. At an early meeting, the

centralization of network management and monitoring was discussed and decided upon [Ref. 3: p. 1].

Management direction of any greater depth was beyond the charter of the CNS. Although the members recognized the importance of this issue, precise instructions to future network managers were nearly impossible to formulate.

5. Assured Internetworking

Since the purpose of the campus network was to provide computer communications support to the whole NPS community, the CNS emphasized the adoption of protocols and techniques which were compatible with all existing departmental sub-networks. Members were concerned that the diverse products being used would preclude communications between the various sub-networks.

For that reason, the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, which has established itself as the dominant internetworking software in the commercial world, was adopted unanimously [Ref. 6: p. 1]. These protocols are discussed in greater detail in Chapter Five of this report.

Additionally, a migration to the International Standards Organization (ISO) Open System Interconnection (OSI) protocols was incorporated into the proposal, and tentatively scheduled for 1991 [Ref. 1: p. 16].

6. Geographical Coverage

Precisely how much of NPS was to be covered by the campus network was also discussed at some length. The "academic quadrangle," bounded by Spanagel, Root, Ingersoll, Halligan, and Bullard Halls was clearly going to be included. But what about the academic support buildings across Fifth Avenue, or the Navy Exchange, or the La Mesa Housing Area?

In determining whether a building or area should be included, the Subcommittee considered the physical limitations of the fiber optic medium, the cost of establishing a network node in an area and the amount of network traffic expected to be generated from that area.

7. Funding

The CNS members realized that although the benefits of the proposed campus network were easy to catalog, such a network would never become a reality if the project was perceived as being too expensive. The Mainframe Replacement Committee had a finite budget to make recommendations on, so each of its Subcommittees, including the CNS, strove to detail the **value** of its own project as well as the **costs** that each proposal were bound to incur.

For that reason, the CNS Final Report contained very detailed price information for its proposed network. These costs were spread over a five fiscal year period, FY-88 through FY-92. Included in this funding schedule were very

detailed cost figures relating to the cable plant, network hardware and internetworking software. The price of the networking project over all phases of the proposed schedule was $875,000 [Ref. 1: p. 14].

This figure included the initial costs of attaching up to ten existing departmental networks to the backbone. The CNS members felt that the success of this number of attached LAN's would establish the viability of the campus network. After the first ten user LAN's are connected and the backbone is operational, additional departments desiring connections would be expected to budget for the hardware and internetworking software needed to attach to the campus net [Ref. 7: p. 1].

F. THE CNS NETWORK PROPOSAL

The following section describes the actual campus network proposal forwarded by the CNS to the Mainframe Replacement Committee. The group's full recommendations are contained in its Final Report, from which the following summary is taken:

> The committee recommends the installation of a campus backbone network to support instruction, research, and administration with the following characteristics:
>
> - Fiber optic token-ring system with an initial data rate of 80 mbps;
>
> - Data rate upgradable to 100 mbps and compatibility with the ANSI Fiber Distributed Data Interface Standard;

- Use of the DoD TCP/IP protocols;
- Ten gateways with multiple ports for connecting to major departmental computer systems;
- One gateway for connecting to off-campus networks and computer systems;
- Teleconferencing capability;
- Management and support structure for both operational support and policy development;
- Funding for connecting ten departmental systems to the backbone (demonstration projects). Departments would fund additional connections. [Ref. 1: p. 3]

1. Network Services

The first section of the Subcommittee Report establishes the usefulness of the proposed network through the 1990's. It lists ways in which the network could aid the instructional, research and administrative work at NPS.

It cites examples of on-going work of specific research departments, including Oceanography and Meteorology. It also lists numerous administrative applications which the network could enhance.

Of equal importance, the Report recommends ways to meet those requirements with commercially available products. The well-established DOD TCP/IP protocol suite was endorsed since it provides three of the most commonly required user services:

- Electronic Mail via the Simple Mail Transfer Protocol (SMTP);
- Remote Login via Telnet;
- File Transfer via the File Transfer Protocol (FTP).

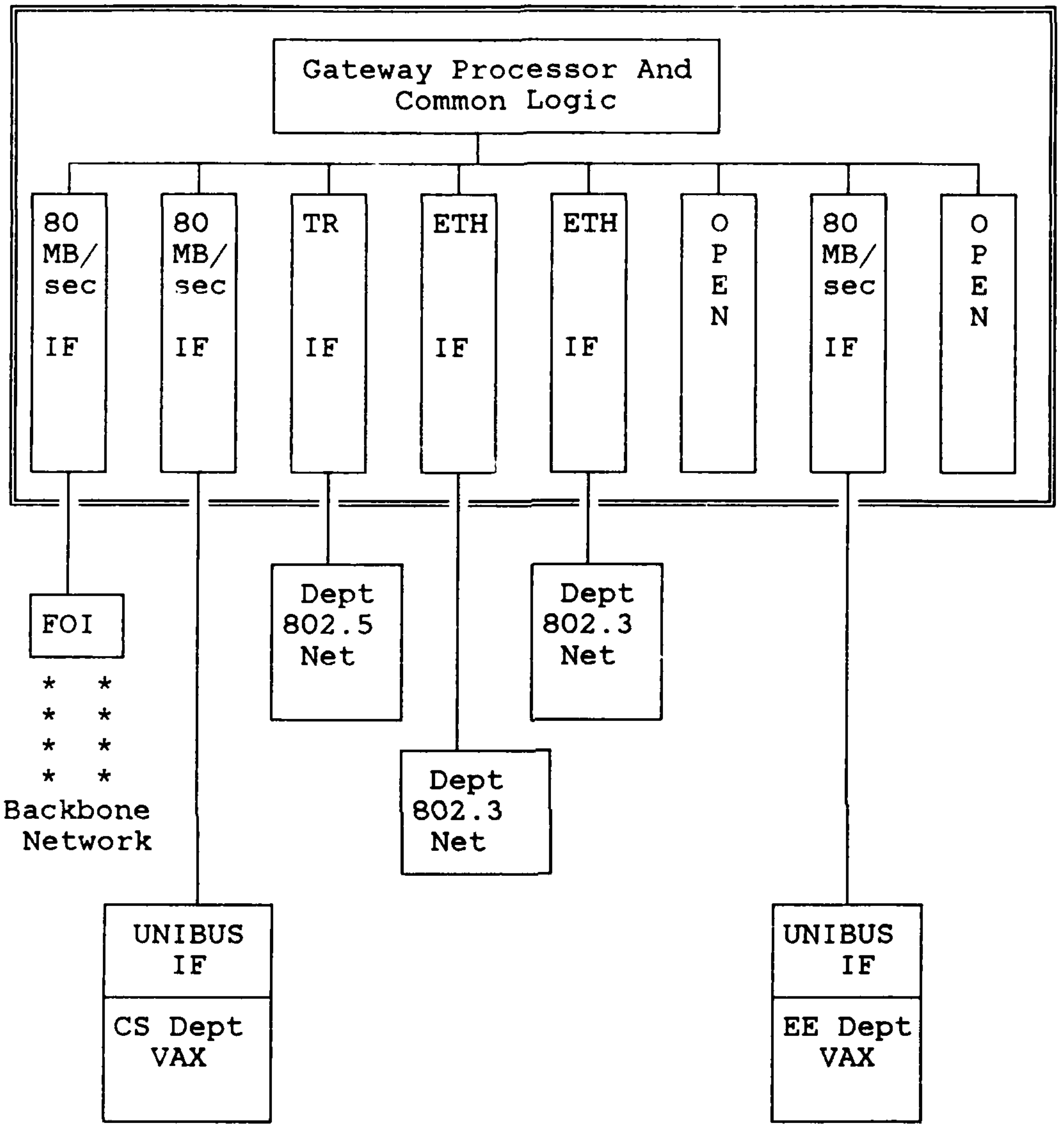
In addition, adoption of the ISO protocols was anticipated, with $33,000 being earmarked for purchase and introduction of the OSI protocols in 1991 [Ref. 1: p. 16].

2. Network Gateways

A gateway is "...a node or station which connects two dissimilar networks." [Ref. 8: p. 28] In the proposed campus backbone network, the gateway converts the data stream from a departmental subnet into a form which is coherent to the backbone. It also performs the reverse process on data from the backbone intended for the subnets.

The gateway node on the campus network would be configured to interface the backbone with all of the different types of subnets supported by that node. The CNS Report recommended the purchase and installation of ten of these gateways.

As an example of how such a gateway would work, let's look at a hypothetical gateway device which could support the Computer Science and Electrical Engineering Departments in Spanagel Hall. Assume that the departments desire to attach two large VAX minicomputers, two IEEE 802.3 (Ethernet) and one IEEE 802.5 (token-ring) networks to the campus net. Each subnet requires its own interface card in the gateway, along with the cabling needed to attach to that card in the gateway. The gateway itself would be attached the backbone network, providing connectivity between all attached subnets and the backbone. Such a gateway is



LEGEND
IF = Interface
FOI = Fiber optic interface
**** = Fiber optic cable
——— = Cable common to subnet

Figure 2.3 Typical Gateway Operation

illustrated in Figure 2.3, which also appeared in the Subcommittee's Report [Ref. 1: p. 15].

3. Network Topology

As was mentioned earlier in the chapter, the placement of the cable was a matter of discussion by the CNS members. The decision was made to make the academic quadrangle the prime focus of the cable plant, since most of the network traffic was expected to be generated there. Backbone access was also provided to Herrmann Hall and to Building 223, which contains a student study area and a portion of the Oceanography Department.

Figure 2.4 depicts the buildings which are to be the sites of the gateway nodes, as well as a possible location of the cable itself. (Please note that the drawing is for illustration purposes, and not intended to specify the precise placement of the node sites or cable runs). As can be seen, the ring established by the backbone cable encompasses those buildings which the CNS members decided would generate the greatest demand for network services.

The maximum distance from which a subnetwork could attach to a gateway node depends on that subnetwork's transmission medium and its signalling technique. Therefore, departmental networks need not be in the same building as the backbone gateway. Moreover, each gateway node listed in Figure 2.4 could attach subnetworks over long

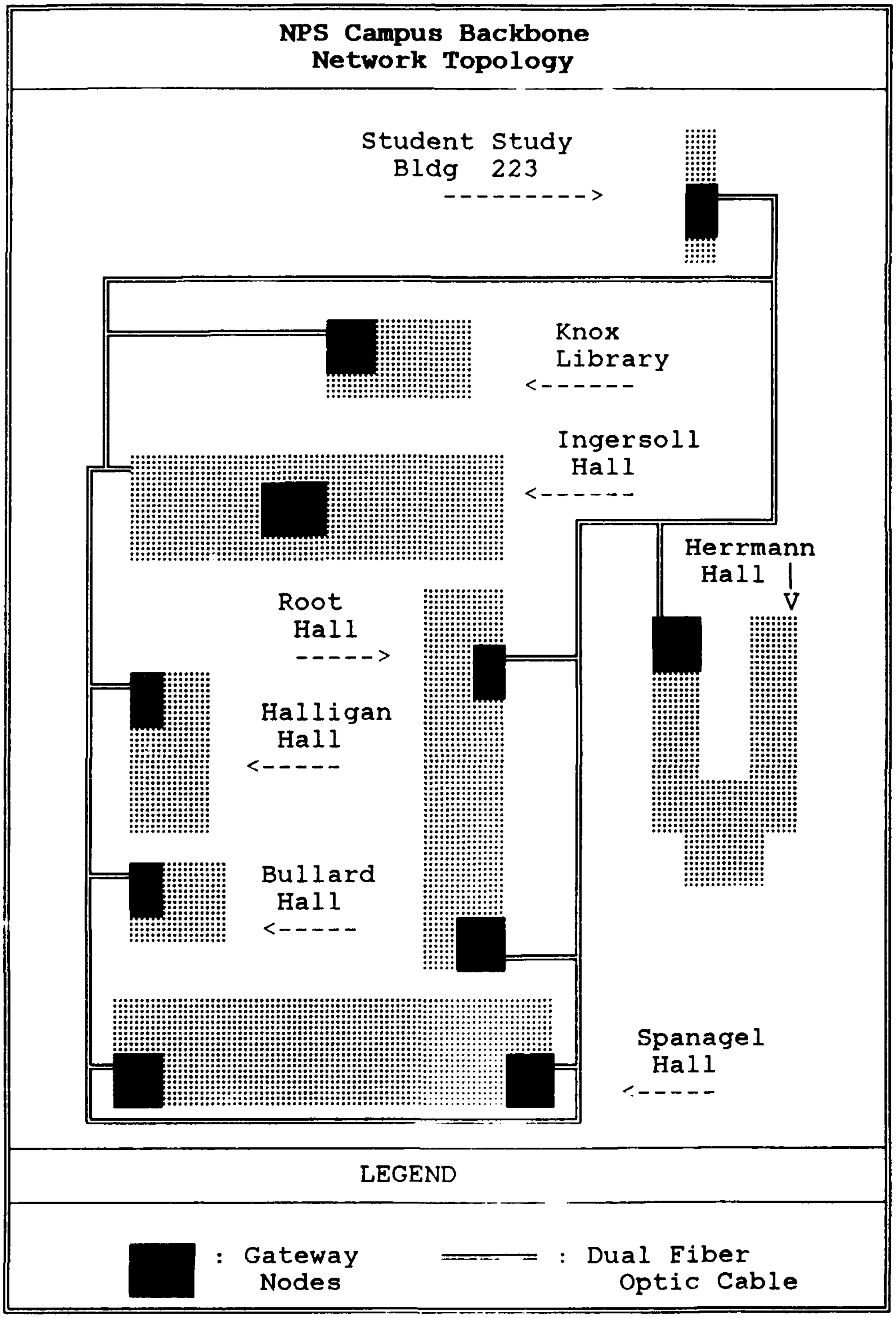


Figure 2.4 NPS Campus Backbone Network Topology

distances, depending upon the characteristics of the attaching network.

4. Network Management and Support

The CNS final report did not include specific direction on the management of the campus network. Instead, it stressed the need for centralized network management in the form of dedicated and experienced computer network professionals. The report also recommended the establishment of a committee whose function it would be to provide campus network policy guidance. [Ref. 1: p. 17]

The following is taken from the final report itself, and sums up the CNS network management recommendations:

- Operational support from competent networking personnel is required for the day-to-day backbone management; and
- That a committee should be formed to provide policy guidance for the planning, implementation and operation of the network. [Ref. 1: p. 17]

G. CHAPTER SUMMARY

In this chapter we looked at the origins and workings of the Connectivity and Networking Subcommittee. The composition of the group was discussed, as were the issues which the group addressed.

Finally, the CNS Final Report was summarized, and each major section of the Report was discussed.

III. THE BASE INFORMATION TRANSFER SYSTEM

One of the CNS working groups sought to determine the NPS user requirements for the campus backbone network. Originally the group members planned to develop a questionnaire for distribution to selected representative users around the campus. They soon learned, though, that the NPS Military Operations Department had already requested this information from all school activities and tenant organizations in conjunction with a Department of the Navy (DON) program called BITS, or Base Information Transfer System. Appendix B of this report contains a copy of the BITS survey.

The CNS working group discussed using the BITS surveys, rather than their own questionnaire, as the basis for their user data. The BITS survey was broader in scope than the questionnaire the group members had envisioned. It sought much more user information than was needed for the CNS working group's purposes. But the group members were concerned that a second "NPS Network" survey would lead to confusion around the campus.

Since the published deadline for submission of the BITS surveys coincided with the group's timetable, the group members decided to forego their own questionnaire and made arrangements to have the BITS data forwarded to the CNS.

The work of the CNS closely paralleled the efforts of the Navy's BITS program. For that reason, the origin and purpose of that program are explained below. Comparisons between the two programs are described later in the chapter.

A. THE BITS PROGRAM

1. The Pre-BITS Navy.

As early as November, 1985, the Chief of Naval Operations, in an Information Resources Management Memorandum (DONIRM) No. 107, recognized that the lack of total LAN planning was causing gross inefficiencies in Base-level data communications. Issues of interconnectivity and interoperability were not being considered by individual offices and departments as they solved their own independent LAN requirements. [Ref. 9: p. 1]

This uncoordinated approach to Automated Information Systems (AIS) caused duplication in time, effort, costs and personnel. Figure 3.1 lists some elements common to communications networks at most Navy stations.

Commanders of most Navy facilities were not aware that the piece-meal approach to AIS and LAN management was sabotaging all efforts at efficient data communications. Education of base commanders was therefore an important aspect of the early DON guidance.

DONIRM No. 107 urged that Base-Wide LAN planning be made part of each Base Master Plan. It also recommended that the LAN plan:

- Use the Defense Data Network for long haul data;
- Consider fiber optic cabling;
- Consider the resources needed for this network in terms of both personnel and equipment. [Ref. 9 : p. 1]

2. July 1986: Additional Guidance

DONIRM No. 71, published in July, 1986, gave commanders at Base facilities more direction for coordinating LAN growth. "Base-Wide Solutions" became the cornerstone of the plan. Each Base was to "package" its data communication requirements and seek the best overall Base-wide solution. The document also urged the Navy AIS system designers and developers to discuss with local users the new systems which will affect Base plans. "Local planning efforts are often hampered by lack of planning information and schedules." [Ref. 10 : p. 1]

3. DONIRM No. 155: Birth of the BITS

Published on 18 December 1986, DONIRM No. 155 was simply titled, "Data Communications Planning." It directed the Naval Data Automation Command (NAVDAC) to develop the procedures needed for establishing an integrated, base-wide telecommunications system at each Navy Base and Station. The project was named the "Base Information Transfer System," and so the BITS effort was begun. [Ref. 11: p. 1-2]

Since the program cuts across many areas of major command responsibility, DCNIRM No. 155 defined the roles of the various organizations involved. Among them are NAVDAC, the Naval Telecommunications Command, the Naval Facilities Engineering Command and each Navy activity, as users.

The stated purpose of the BITS is both far-sighted and encompassing:

> The BITS effort will implement ... a single system to support all current and foreseeable future requirements for data, voice, and video communications, plus physical security equipment for approximately the next twenty years (1990 through 2009). [Ref 11: pp. 1-1]

Figure 3.2, from [Ref. 11] illustrates these objectives of the BITS program.

B. IS THE BITS POSSIBLE?

The program is very broad in scope, and places a premium on a comprehensive approach to communications needs. No longer could a telecommunications manager focus only on phones and messages, nor the AIS manager focus only on data. The lines dividing these two disciplines are blurring throughout the Navy.

The very breadth of the BITS program, as described above, may prove to be a limitation during the early years of the program's development. At present there are no commercially available networking products which could provide all the applications listed. For instance, the Integrated Services Digital Network (ISDN) standard, which

allows the mixed transmission of voice, data and video over the same network, is gaining acceptance in many commercial sectors. However, ISDN is not used yet over very high speed fiber optic cable plant. Also, specification of the ANSI Fiber Distributed Data Interface (FDDI) Standard, which would establish communications protocols for very high speed (100 MBps) fiber optic cable, is only now nearing completion. But even after the protocol is specified, there will still be a lag before FDDI products become "plain off-the-shelf" commodities. Although technologies such as these tend to mature rapidly, their wide-spread availability in the early 1990's is questionable.

C. IMPLEMENTING THE BITS PROGRAM

Less than six months after DONIRM No. 155 directed the adoption of the BITS Program, NAVDAC proposed an implementation program, divided into five action phases. The BITS timetable as devised by NAVDAC is listed in Figure 3.3, including the actions required in each of the phases.

Note that these phases extend through the entire life-cycle of the project, to include the long maintenance period which follows the actual installation of the network system [Ref. 11: p. 3].

The NAVDAC instruction also outlines the responsibilities of the Base "Point of Contact" (POC) for BITS. DONIRM No. 155 required that each base establish and

staff this billet, and instructed NAVDAC to assign specific duties to the individual. As the Base Commander's BITS resident expert and project officer, the POC is responsible for the local planning and execution of the program. For that reason, it was "recommended" that the base telecommunications officer be assigned to the POC billet. [Ref. 12: p. 2]

NAVDAC provided each POC with a user's manual for initiating the program at his base. The manual's "cookbook" format is full of checklists and recommendations for the more effective ways for the POC to accomplish his tasks.

Portions of the POC's job are very complicated, and NAVDAC recognized that some of these tasks require expertise in areas where communications officers rarely gain experience. For instance, the development of the Mission Element Needs Statement, required during the first phase of BITS, is not something that communications officers deal with often. Yet the techniques used in the NAVDAC manual take the POC step-by-step through the creation of that document. This helpful direction is available to the POC through each phase of the BITS implementation, from compiling the survey data to developing the Program Objectives Memorandum.

The checklists contained in the user's manual are also very useful to the POC for regulating the headway he is making. As he checks off each completed action, he is able

to monitor progress. Moreover, each POC sends "Status Reports" to NAVDAC throughout the program, using these same "checkpoints" as points of reference. So formalizing the POC's checklist allows NAVDAC a standardized way of monitoring the program at all Navy installations.

In summary, DON recognized a serious problem in base networking, set up general guidelines for a solution, and directed NAVDAC to carry out that solution. In turn, NAVDAC established milestones and concrete procedures to be followed at each Navy installation.

D. THE NPS BITS IMPLEMENTATION

1. NPS: A Unique Activity

Introducing the BITS at NPS has proved difficult to date, primarily because the School is unlike the "typical" Navy base to which NAVDAC tailored its procedures.

NPS is responsible for the implementation of the BITS for all Navy activities in the Monterey area, as well as other non-Navy NPS tenant organizations. As an example, the Fleet Numerical Oceanography Center (FNOC) is one such Navy command. The Defense Manpower Data Center (DMDC) is an example of a non-Navy tenant organization for which NPS is responsible. Accordingly, NPS cannot exercise the immediate control over all the network participants that a typical activity could.

But within the Naval Postgraduate School's own organization there are characteristics which make it unique. In addition to the command and staff structure which one finds on every base, there is also an academic structure with its own rankings, goals and priorities.

The research functions that the School performs also put NPS in a category of its own. The size and complexity of the computing devices used to support this research create specialized networking difficulties which are probably not seen at other bases.

Finally, there is the security issue. NPS has no armory or ammunition storage facilities. No nuclear powered ships dock here. No expensive aircraft line its runways. So the emphasis that the BITS places on networked physical security support is not of as great a value to NPS as it would be at other Navy facilities.

2. Designating the Point of Contact

As mentioned earlier, DONIRM No. 155 recommended that the telecommunications officer be assigned as the BITS POC if possible. [Ref. 12: p. 2] This recommendation was not heeded at NPS for many reasons. It was originally decided that the POC would be the Director of the Computer Center, in recognition of the importance of computer communications at the School. At a later point the POC duty migrated to the Assistant Military Operations Officer, who

maintained liaison with the Computer Center staff for clarification of technical issues.

3. Distributing the BITS Surveys

During September 1987, the surveys were sent to all activities under the cognizance of NPS. A cover letter to the survey form amplified the instructions contained on the survey itself. Each activity was required to complete a form for each building in which it maintains an office. The completed surveys were to be returned to the Military Operations Office by 15 October. [Ref. 13: p. 1]

4. Compiling the Results

The surveys were not all returned until early December. Computer Center personnel then standardized the responses, and created all of the required summary reports. These reports were forwarded to the NPS BITS POC as enclosures to [Ref. 14]. As of this writing, NPS has completed Phase 0 of the BITS implementation plan.

E. BITS AND THE CNS PROPOSAL COMPARED

In Chapter 2, this paper addressed the Campus Network proposed by the CNS. In the previous sections of this chapter, we discussed another Navy-directed network plan, the BITS. How are these plans coordinated? How do their functions compare? Figure 3.4 compares important aspects of the two proposals. This section will briefly deal with these issues. Because the BITS program has not reached the point

of defining technical specifications in all areas, some of the characteristics listed in the figure and discussed below cannot be confirmed from the BITS literature. Instead, they are based on expected trends in high capacity fiber-based local area networking.

1. Protocols

Both networks will use the ANSI FDDI protocols to implement their fiber optic medium. These protocols are discussed elsewhere in this paper. For internet and transport services, the CNS network specified TCP/IP due to its growing acceptance in the late 1980's. The BITS will probably require the use of the ISO internet combination, TP-4/IP, since the Federal Information Processing Standard (FIPS) will have been put into effect by the time the BITS is ready for installation [Ref. 15: p. 1].

2. Cable Plant

Both systems will use fiber optic cable meeting the specifications of the ANSI FDDI standard.

3. Services Provided

Since TCP/IP will be used on the CNS campus net, users will have electronic mail, file transfer and remote login (telnet) capability across the network. The BITS literature promises a multitude of services, ranging from electronic mail to vi‹ ɜo broadcasts. It is difficult at this to envision how this would be implemented.

4. Coverage

Chapter 2 described the area covered by the CNS proposed network. It is not necessarily available to all locations aboard the NPS campus, and does not include any plans to extend to the FNOC facilities. Its primary foci were the academic area between Spanagel and Ingersoll Halls, and the administrative offices in Herrmann Hall.

BITS, on the other hand, places a premium on its totality. It is expected that BITS will cover not only all of the NPS campus, but the FNOC facility, tenant organization sites, and the La Mesa Housing area.

5. Technology Availability

The Campus Network Subcommittee discussed technical feasibility and availability at great length. The group placed a premium on specifying performance from proven technology. In the case of the FDDI standard, operational high speed fiber-based networks have actually been fielded, very similar to the form that the ANSI standard will take when it is fully adopted. So the CNS designated protocols, hardware and software which are available virtually "off the shelf." For that reason, it is fair to say that the CNS network could be installed by 1990.

The same cannot be said about the BITS. The integrated services which it promises require a technology which has not yet been commercially adapted to a high speed

fiber optic network. For that reason, full operation cannot be expected until at least the early 1990's.

6. Complementary Systems

The CNS campus network should be viewed as the precursor of the full BITS program. Since the fiber optic cable plant will be common to both systems, the BITS net, when it is ready for introduction, could be superimposed onto an already operational campus network. The BITS system would be an upgrade or expansion of the existing campus network, rather than a entirely new enterprise. The campus network could be absorbed into the BITS net.

For that reason the CNS-proposed campus network could serve as a valuable testing ground for the BITS. This would help the BITS in a number of ways. First, by the time the BITS becomes operational in 1992 or beyond, NPS campus net users will have been exposed to the benefits and difficulties related to a large multi-departmental networking systems. Second, NPS network personnel will have gained experience with the fiber optic medium; and with the technical and managerial problems that fiber creates.

Therefore the two networking proposals should not be thought of as mutually exclusive enterprises. Instead, they are complementary systems which address different problems during different time frames.

F. CHAPTER SUMMARY

In this chapter we looked at the Navy's plan for attacking the inefficiencies which characterize the DON data communications plans. The formation of the BITS Navy-wide, and the initiation of the program here at NPS were described. Finally, the relationship between the CNS network and the BITS was characterized as being complementary.

IV. FIBER OPTICS IN LOCAL AREA NETWORKING

Stallings calls the development of practical fiber optic communications systems, "...one of the most significant technological breakthroughs in data transmission." [Ref. 16: p. 51] Other observers are even more ecstatic, calling the growing use of fiber optics "revolutionary," and warning managers and designers to "...be careful not to get trapped by old thinking," in their cable plans [Ref. 17: p. 27]. The adoption of the optical fiber medium by large LAN planners such as the CNS in its Campus Network Proposal (Chapter 2) and the Department of the Navy in its BITS Program (Chapter 3), affirm the arrival of practical fiber optics systems.

The purpose of this chapter is to familiarize the reader with the basics of optical fiber communications systems, and the way that the ANSI FDDI standard will exploit the speed and reliability of these systems for high bandwidth LAN's.

A. BRIEF HISTORY OF OPTICAL COMMUNICATIONS

In a broad sense, human beings were communicating with light long before they used electrical current. Consider smoke signals, torches and reflected sunlight as some of the earliest examples [Ref. 18: p. 4]. Even in today's technologically sophisticated world, semaphore signalling

between ships at sea is a comparatively secure means of communication sometimes preferred by Navy commanders.

Transmitting light through a medium also has ancient origins. Glass was used to transmit light in ancient Greece, and water was used as a transmission medium in nineteenth-century England. A cable similar to the present glass fiber, consisting of a glass core coated with another glass material, was experimented with in England in 1958. But very high transmission losses over short distances caused interest in fiber media to wane. [Ref. 18: p. 5]

But the development of the **laser** in 1960 provided experimenters with their first coherent (single color) light source. Rather than the light which was prone to dispersion over distance, the laser provided "...a superradiant beam of narrow bandwidth." [Ref. 16: p. 55] Suematsu and Iga describe the resurgence of excitement among the scientific community:

> Initially it was thought that a communications system operating at optical frequencies would increase the information-carrying capacity by as much as 100,000 times compared with existing systems [Ref. 18: p. 2].

However, there were many problems which had to be addressed before practical laser systems were possible. The late-1960's saw scientists developing smaller and more efficient lasers, high-speed modulation and demodulation devices, and flexible, economical high-speed optical fiber.

Marrying the twin developing technologies of practical semiconductor lasers and more efficient optical fibers, English laboratory scientists in the early-1970's announced a full Gigahertz (GHz) bandwidth transmission over a one kilometer distance [Ref. 18: p. vi]. Fiber optic communications were on the verge of practical reality. By the late-1970's, trial systems were being installed and tested in the United States, England, Japan and Italy. New bandwidth records (32 MBps, 34 MBps, 44 MBps, 140 MBps) were established on a regular basis [Ref. 19: p. 290].

By 1987 fiber had replaced metal cables on many of the large volume links in U.S. wide area networks. And the trend was clearly toward more and faster fiber optic lines. During that year, AT&T brought operational billion-bit-per-second transmission to the United States for the first time with a 1.7 Gigabit per second (GBps) fiber optic link between two Illinois central offices [Ref. 20: p. 36].

Recently, manufacturers began developing relatively inexpensive fiber optics products for local area networks. These products are mostly lower speed (2, 4 and 10 MBps), and oriented toward the users who need higher reliability and longer distances than conventional LAN architectures would provide [Ref. 20: p. 262]. However, much faster (100 MBps) fiber optic LAN's are expected to grow in popularity after the FDDI specification process is completed.

B. COMPONENTS OF OPTICAL COMMUNICATIONS SYSTEMS

1. The Fiber Optic Cable

The speed advantage that optical communications enjoys over other electrical forms of transmission, such as telephones, satellites and radio derives from the higher frequencies at which visible light travels. The frequency is higher, and the wavelength is much narrower: on the order of one micron in width. (Appendix C contains a chart showing the relative frequencies and wavelengths of the electromagnetic spectrum, taken from Suematsu and Iga).

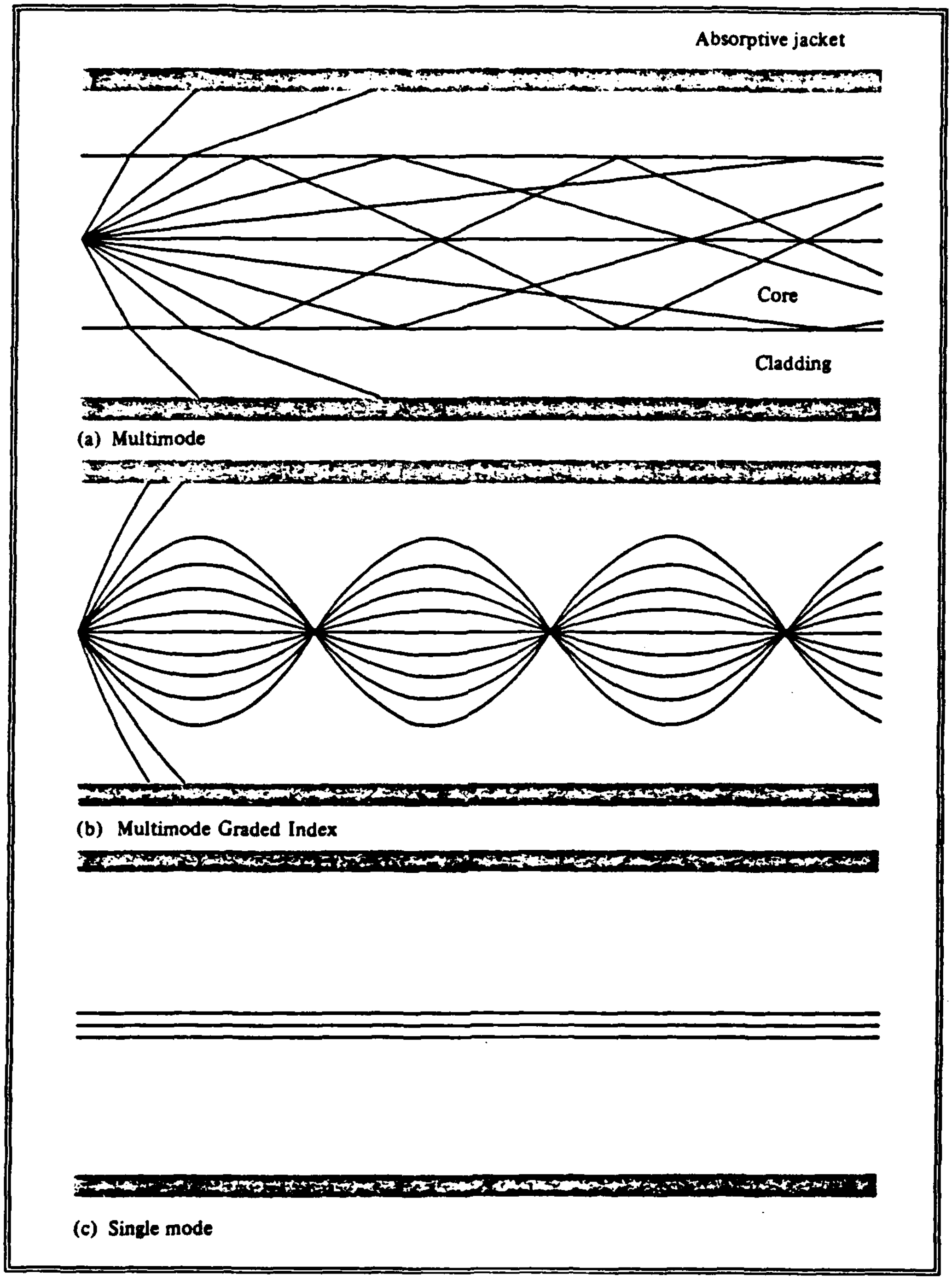
The challenge to the cable designers is to keep the light wave from becoming distorted, by keeping the wave focused on the emitted wavelength. Ideally, the core of the cable is very narrow, as close to the size of the desired light wave (the axial ray) as possible. Rays that are of lower frequency and larger wavelength would be either reflected inward toward the axial ray, or be absorbed by the core covering, called a cladding.

A parallel is drawn with basketballs being shot down a pipe. If you wanted the balls to exit the pipe in a steady stream, you would try to keep the pipe as close to the diameter of the basketball as possible. If the pipe were much larger than the balls, as in a culvert pipe, the balls would ping-pong down to the destination and exit in splatter-gun fashion. [Ref. 21: p. 262]

Figure 4.1 illustrates three of the optical fiber transmission modes. In 4.1(a), a **multimode cable** is shown. Multimode fibers contain a relatively large core, and allow for a range of wavelengths to be transmitted, with the axial ray at their center. The cladding disperses rays entering at very diffuse angles, thereby preventing massive distortion of the axial ray.

An improvement on the standard multimode fiber incorporates a "re-focusing" characteristic. Referred to as **multimode graded index**, this type of cable is shown in Figure 4.1(b). As with all multimode fiber, the cladding absorbs rays entering at extreme angles. But by taking advantage of varying (graded) indices of refraction in the fiber itself, the cable tends to re-focus rays back toward the optimal wavelength.

Figure 4.1(c) illustrates the **single mode** or **monomode** fiber. Here the core radius is reduced to the order of the wavelength. So only a single angle or mode can pass [Ref. 16: p. 53]. It is the monomode cable systems which set the fiber speed records, as in the Illinois AT&T 1.7 GBps link mentioned above. This speed is achieved by channeling the very high frequency optical wave down a very narrow waveguide. Instead of basketballs down a drainpipe, the monomode cable systems have more in common with a bullet down a rifle barrel. Very high speed and no alternative directions but straight ahead.



From Stallings: Data And Computer Communications

Figure 4.1 Three Optical Fiber Transmission Modes

Figure 4.2 is taken from Stallings [Ref. 16: p. 54] and makes practical comparisons between the monomode and multimode fibers.

For the reasons listed above, monomode cable has become the choice for long-haul, high volume, point-to-point communication networks. Multimode cable has made inroads in smaller systems, including LAN's, where many taps to the fiber media are required.

In general, the fiber optic cable market seems destined for continued growth. In 1987 U.S. fiber cable sales reached $589.9 million, or 20.3% of the total wire and cable market. Cable manufacturers expect such sales to grow 10.7% annually for the next five years to $1.07 billion in 1992. [Ref. 22: p. T6]

2. The Light Source

Multimode fiber can be used with two types of light transmitters: lasers and light-emitting diodes (LED). Lasers are more powerful, and have narrower spectral widths than LED's. So lasers have the potential for much higher signalling capacity. But LED's are simpler, cost less, consume less power, and still support bandwidth in excess of most local network requirements. [Ref. 23: p. 20]

C. ADVANTAGES OF OPTICAL COMMUNICATIONS SYSTEMS

Figure 4.3 lists some of the advantages which fiber optics media offer to communications managers. Each of

Single Mode	Multimode
Used for:	Used for:
- Long Distances	- Short Distances
- High Data Rates	- Low Data Rates
Expensive	Inexpensive
Narrow Core	Wide Core
Requires Laser Source	Can use LED Source
Hard to Terminate	Easy to Terminate
Minimum Dispersion	Large Dispersion
Very Efficient	Inefficient

From Stallings: Data and Computer Communications

Figure 4.2 Comparison of Single Mode and Multimode Optical Fiber

Advantages of Fiber Optics Media in Communications
* Very High Bandwidth
* Low Signal Attenuation
* Relative Security
* No Electromagnetic Interference
* Light Weight
* Low Cost

Figure 4.3 Advantages of Fiber Optics Media in Communications

these optical fiber advantages will be addressed in the following section.

1. Very High Bandwidth

The high speed of fiber optic links is certainly one of its most highly regarded benefits. Networks are now operational at 1.7 GBps. In November, 1987, laboratory experimenters using very sophisticated devices achieved 27 GBps [Ref. 24: p. 65]. In LAN's, the FDDI specification will standardize a 100 MBps system, and plans are already in the works for another system, FDDI-II, which will provide even higher speed.

2. Low Signal Attenuation

Fiber optics is a very efficient communications means, in that it loses relatively small amounts of its signal power over distance. As a result, the distance between repeaters in a fiber optic network is greater than it is for metallic media networks. For comparison, Suematsu and Iga claim that a 400 MBps Phase Code Modulated network implemented in coaxial cable would require repeaters every 1.5 km. The same capacity could be achieved on a multimode fiber network with repeaters every 4.5 km. By using monomode fiber, the signal attenuation would be so low that repeaters would only be needed every 25 km. [Ref. 18: p. 164]

3. Relative Security

The unauthorized interception of a network signal is generally done in two ways: 1) physically tapping the cable, or 2) monitoring the emissions from the cable without penetrating it.

Tapping into fiber cable is a difficult procedure. The amount of light energy passing through the medium is measured precisely, so inserting an unauthorized tap would bring down the whole link. And since optical cables don't "leak," or radiate, their signal through the cladding, there are no emanations for an unauthorized agent to detect. This feature of fiber optics is of particular interest to the Department of Defense. Fiber optic cables play a major role in voice and data communications systems approved under the TEMPEST (Transient Electromagnetic Emanations Standard) criteria because they radiate their light only at the ends of connectors. [Ref. 21: p. 260]

4. No Electromagnetic Interference

Fiber optic cable is immune to interference from sources such as power lines, electrical motors and other communications media. For that reason, optical communications are valuable in power plant monitoring systems, or for communications in factories using heavy machinery.

The military is very interested in this aspect of fiber optical communications, because future battlefield

environments will likely be heavily irradiated. Experiments with optical cables in a "high radiation environment" at the Nevada Nuclear Test Site, "...proved their ability to withstand the difficult environment in addition to providing critical performance advantage over coaxial cable." [Ref. 25: p. 1318]

5. <u>Light Weight, Small Size</u>

The core of the fiber cable is literally microscopic. Even when the cladding and protective coverings are added, the cable is still of very fine dimensions. In terms of weight, fiber cables weigh only about 11 percent as much as copper cables of similar width [Ref. 21: p. 262], and their small bulk can free valuable space in crowded wiring closets.

6. <u>Low Cost</u>

The cost of optical fiber has fallen significantly since 1984, and is expected to continue to drop as optical cable fabrication techniques mature. Plastics are being developed to replace the glass which has been the mainstay in optical cable. This should also place downward pressure on fiber prices. Recognizing the decrease in prices, Joshi claimed that "...fiber is projected to become cheaper than coaxial cable in a year or so." [Ref. 26: p. 8]

D. THE FIBER DISTRIBUTED DATA INTERFACE (FDDI)

1. Background

FDDI is a standard being defined by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X3T9.5 for a 100 MBps token ring using an fiber optics medium.

This ANSI effort is a complement to the work of the IEEE 802 committees. Under the terms of a 1982 agreement, the IEEE body will develop standards for networks with bandwidths below 50 MBps. The ANSI X3T9.5 will do the same for networks with speeds exceeding 50 Mbps. [Ref. 27: p. 10]

Originally FDDI was envisioned as:

> ... a packet switching network with two primary areas of application: first, as a high performance interconnection among mainframes, and among mainframes and their associated mass storage subsystems and other peripheral equipment and second, as a backbone network for use with lower speed LAN's such as the IEEE 802.3, 802.4 and 802.5 [Ref. 27, p. 10].

Burr adds that in addition to these technical features, the FDDI Subcommittee members conceived that inexpensive system implementation, was also a worthy goal. Network links were specified which could be designed with relatively inexpensive components which were commercially available in 1986. "No interface standard can succeed until it can be inexpensively implemented." [Ref. 23: p. 9]

After many months of work, the FDDI network as developed by the X3T9.5 Committee is on the verge of being adopted as a full-fledged ANSI standard. The Committee's

proposal takes the form of the draft FDDI-I specification, which is oriented more towards computer data communication than to voice traffic. FDDI-II, a planned enhancement of the original specification, will someday provide a better interface for both voice and data traffic [Ref. 26: p. 8]. For the purposes of this paper, the discussion of FDDI is limited to the FDDI-I standard.

2. The FDDI Documents

The FDDI specification is contained in a set of four documents. These documents are:

- The **Physical Medium Dependent** (PMD) Standard defining the cable, connector and optical transmitter-receiver characteristics.

- The **Physical Layer Protocol** (PHY) Standard handling clock synchronization, coding and decoding and clock recovery;

- The **Media Access Control** (MAC) Standard which specifies a deterministic, timed token protocol guaranteeing network access to each station on the network;

- The **Station Management** (SMT) Standard defining the station and network management operations of each FDDI node. [Ref. 28: p. 38]

Each of these standards will be discussed later in this chapter.

Collectively these standards perform all functions required for the physical layer and data link layer protocols of the seven-layer Open Systems Interconnect (OSI) model. Figure 4.4 is taken from Joshi [Ref. 26], and maps the FDDI documents to the two OSI layers.

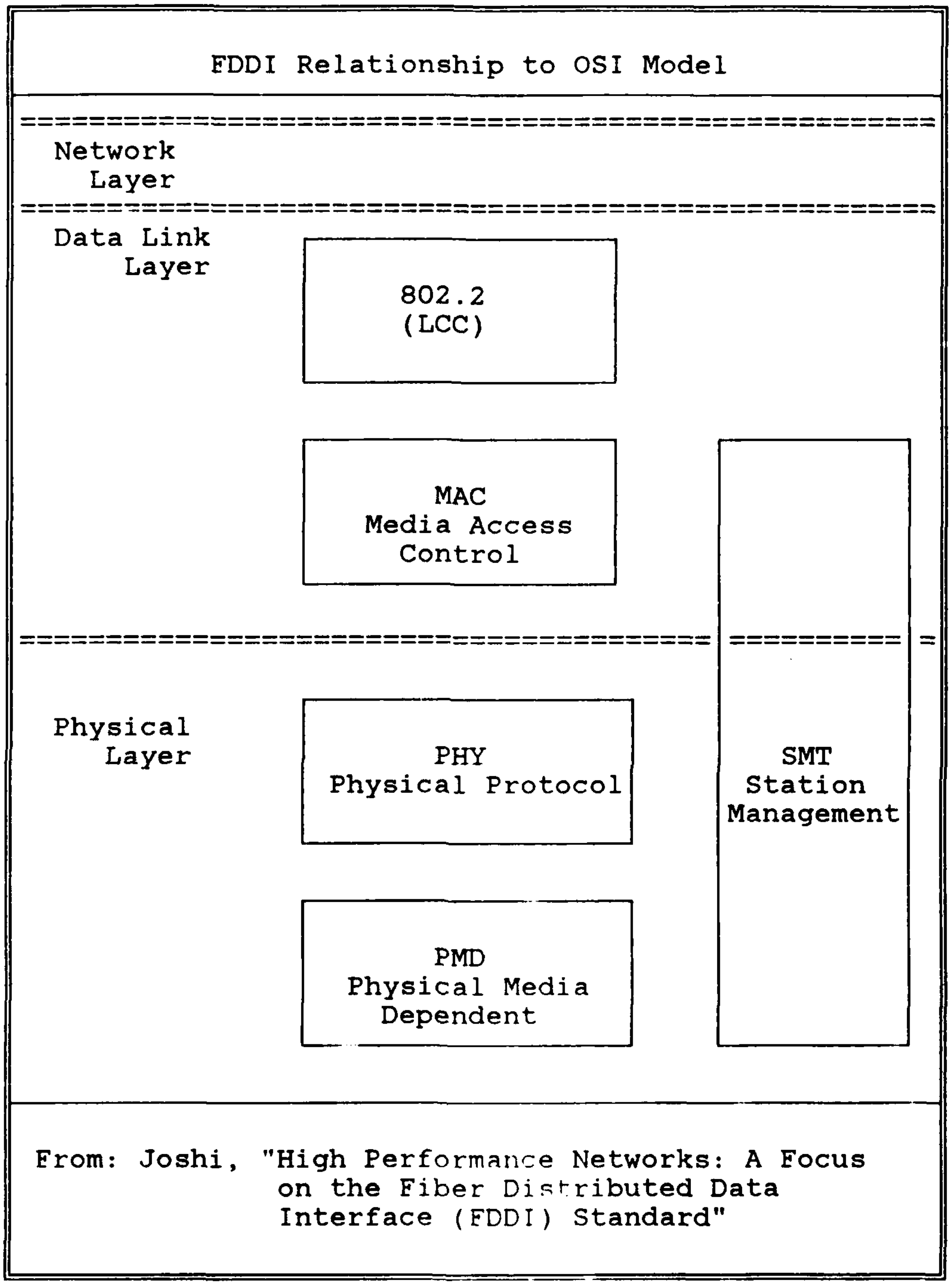


Figure 4.4 FDDI Relationship to the OSI Model

3. The FDDI PMD Specifications

a. The PMD Cable Plant: Multimode

The X3T9.5 Committee's initial network design goals were twofold: 1) 100 MBps speed; and, 2) a minimum two kilometer station-to-station distance. To achieve these two goals, it was clear that fiber optical cable would be the Committee's choice of network medium. But the choice of fiber cable mode was not as clear cut. Monomode fiber would provide higher bandwidth with less attenuation over distance; but monomode transmitters, switches and connectors are all more costly, and more difficult to install and maintain. Graded-index multimode cable allows for easier handling, switching and coupling, and its bandwidth potential still exceeded the X3T9.5 design goals. For that reason, the graded-index multimode cable with a core/cladding size of 62.5/125 microns was specified in the PMD document [Ref. 29: p. 5]. For readers interested in more detail on the Commitee's choice of cable, Burr's article is suggested [Ref. 23: p. 9].

b. The PMD Light Source: LED

The FDDI PMD document was written to allow for the use of LED's as the light transmitters on the network. Although lasers generate more optical power, they were seen as being too costly and prone to failure to be specified on a backbone network consisting of hundreds of light sources.

And LED's which produce the 1300 nm wavelength prescribed by the system are commercially available . [Ref. 23: p. 21]

It is interesting to note that the PMD does not **preclude** the use of laser devices on an FDDI-compliant network. Rather, it specifies performance which does **not require** the power of the laser. Therefore a network manager could consider the user of laser transmitters between stations that exceed the FDDI minimum distance of 2 km, and less costly LED's in the remainder of the stations on his network.

> ...the PMD is written to allow the use of LED's. Still, lasers can also clearly meet PMD specifications, and could offer greater link distances, while preserving compatibility with all stations at distances of less than 2 km [Ref. 23: p. 21].

c. The PMD Light Detector: PIN Diodes

Two types of light detectors are currently in commercial use, PIN diodes, and Avalanche Photo Diodes (APD). Although APD's have greater signal sensitivity, the X3T9.5 Committee members were concerned that APD's in the 1300 nm wavelength were not available as "commodity products." Therefore the less sensitive PIN diodes were specified, "...because of the component availability and cost goals of FDDI." [Ref. 23: p. 21]

3. The FDDI PHY Specification

a. Frame and Token Formats

The FDDI specification calls for two types of packets to be used on the network, an information frame

consisting of nine fields, and the token frame, consisting of four. Figure 4.5 illustrates the formats for the two types of frames.

b. Signal Clocking

The high speed of the network mandates clocking precision of the highest order. Bit cells during network transmission have a period of 8 ns, a remarkably brief time! This means a deviation (jitter) exceeding 4 ns will create a bit error [Ref. 23: p. 22].

The preamble (PA) field of each frame precedes each transmission stream, and is used for establishing and maintaining clock synchronization. The PHY specification also requires that each station maintain a 10-bit "elasticity buffer" which allows the receiving station to adjust its timing while synchronization is being achieved with the sending station.

c. Coding and Decoding: 4B/5B

Unlike lower-speed standards which use Manchester encoding for baseband transmission, the PHY document directs that the more efficient 4B/5B scheme be employed. Since 4B/5B performs at 80% efficiency, instead of Manchester's 50%, FDDI can exact a 100 MBps data rate from a 125 MBaud rate on the fiber medium [Ref. 26: p. 13, and Ref. 27: p. 11].

Information Frame

PA	SD	FC	DA	SA ----->

-------->	Info Field	FCS	ED	FS

Token Frame

PA	SD	FC	ED

Legend

PA = Preamble
SD = Starting Delimiter
FC = Frame Control
DA = Destination Address
SA = Source Address
FCS = Frame Check Sequence
ED = Ending Delimiter
FS = Frame Status

From: Ross, F. E., "FDDI - A Tutorial," Ref. 20.

Figure 4.5 FDDI Frame and Token Formats

4. <u>The FDDI MAC Specification</u>

The function of the MAC specification is to allow for any station to determine "...which station has control of the medium, and what is to be placed on the medium." [Ref. 27: p. 13] It manages copying, stripping and addressing frames, capturing the token frame when needed, and error control.

a. Copying Frames

Each station captures and repeats the frame it receives. If the destination address (DA) of the frame that it receives is its own, then it copies the frame into an input buffer, and marks the FS field as copied.

b. Stripping Frames

If the station has transmitted frames, it monitors its incoming traffic for those frames which have its own address as the source field (SA) and a "copied" notation in the FS field. If it finds such a frame, it strips it from the network.

c. Addressing Frames

MAC also manages the address fields SA and DA, which can be 16 or 48 bits in length. MAC determines address field length by an identifier in the FC field. [Ref. 27: p. 13]

d. Token Capturing

If MAC has traffic from either the LLC or SMT layers to transmit, it must wait until it captures the

network token, a special frame which entitles a station to transmit. Once it has completed its transmission, the MAC will insert a new token onto the ring. [Ref. 27: p. 14]

e. Data Integrity Check

The Frame Check Sequence (FCS) field contains 32 bits and is used to verify the integrity of the incoming data stream by means of a cyclic redundancy check.

5. <u>The FDDI SMT Specification</u>

SMT exercises overall control of all station activity by managing the following functions:

- higher level address administration;
- allocation of network bandwidth;
- network control and reconfiguration [Ref. 27: p. 15].

a. Station Types

FDDI recognizes two classes of network stations. **Class A stations** connect to both of the network's counter-rotating rings at once. The redundancy of the second ring enhances the Class A station's survivability in the case of a cable failure. A **Class B station** attaches to only one of the rings. Accordingly, a Class A station will have twice the protection against cable interruption that a Class B station will have. [Ref. 26: p. 11]

b. Network Reconfiguration

The fault tolerance afforded each Class A station is one of the most promising features of the FDDI specification. Component failures are "sensed" by the

network almost immediately, and the SMT in each station establishes alternative data paths. "In FDDI, this reconfiguration happens...within a few milliseconds." [Ref. 26: p. 12]

c. Timed Token Rotation (TTR) Protocol

In conjunction with the MAC, the SMT allows for prioritization of token requests on the network. The TTR Protocol is employed to guarantee a minimum response time on the ring. SMT brokers a type of "node bargaining," in which a station "bids" on the amount of traffic that it will be allowed to send the next time it captures the token. If there is little traffic on the net, few stations will challenge another station's request for priority service. Under heavy loads, however, the net will be honor fewer priority requests, since such requests will jeopardize the minimum response time guarantee. [Ref. 26: p. 13]

E. FDDI PRODUCT AVAILABILITY

A good deal of divergent speculation revolves around the question of FDDI-compliant product availability. The standard itself is still in the process of gaining full ANSI accreditation, with completion expected in the third quarter of 1988 [Ref. 30: p. 15]. But draft copies of the MAC, PHY and PMD documents have been available to manufacturers since late-1986. And manufacturers have incorporated the specifications into a number of FDDI-like products,

promising a "clear migration path" to FDDI compliance when the complete standard is available [Ref. 31: p. 13]. Among the companies offering such products are Fibronics Corporation of Hyannis, Mass., and Proteon Incorporated, of Westborough, Mass. [Ref. 32: p. 7]

Optimists speculate that full implementations of FDDI-compliant products will be available in 1989-1990 [Ref. 29: p. 6]. Skeptics argue that the complexity of the FDDI systems require more study, development, engineering and training than was the case with any previous network standards implementation (as in any of the IEEE 802 networks). They contend that 1990 is too soon to expect a system implementation, since a 1990 schedule would leave "...little margin for error." [Ref. 31: p. 13] A more realistic date, skeptics claim, would be late-1991.

In either event it seems certain that once adopted the FDDI standards will impact local area networking well into the next century.

E. CHAPTER SUMMARY

Fiber optics communications is fundamental to the implementation of the proposed NPS Campus Network. Accordingly, this chapter was devoted to a brief explanation of optical communications and its effect on LAN's.

The section began with a quick look at the history of fiber optical communications. The features which make fiber

optics so attractive to local area network planners were then discussed. How the FDDI protocols will tame the vast potential of the fiber medium was then addressed. Finally, the availability of FDDI products was explored.

V. INTERNETWORKING ON THE CAMPUS NETWORK

Miller, in proclaiming 1986 as "The Year of Networking," asserts that one loud and clear message is being heard from users of both local and wide area networks. That message is: "Users want multivendor, interoperable networking systems." [Ref. 26: p. 6] Not satisfied with having similar devices communicating on a single network, users are now demanding connectivity between networks. Getting computers to communicate across a variety of hardware suites, operating systems and communications networks has been the goal of networking engineers and designers for years. But now as we approach the 1990's this goal is becoming a reality.

Internetworking is a critical component of the Campus Network Plan. The BITS surveys identified 57 LAN's which were either installed or planned for installation at NPS and its subordinate organizations [Ref. 14]. Included in those 57 LAN's are products from virtually every major network vendor. The FDDI fiber backbone net will offer the physical connection between any of these LAN's in the form of data streams. But such a backbone would be of little use without the means of "translating" the source subnetwork's bit streams into patterns that are meaningful to the destination

subnetwork. This translation is the responsibility of the internetworking protocols.

In this chapter we will study the purpose and functions of protocols in more depth, then look at two celebrated internetworking protocol suites: DOD´s TCP/IP and ISO´s OSI. Finally we will discuss the strategy used in choosing the internetworking protocols to be used on the Campus Network.

A. PROTOCOLS: CHARACTERISTICS AND FUNCTIONS

Simply stated, networking protocols are the "rules of the road" used to effect meaningful interaction between computer systems. Stallings stated it as follows:

> What is communicated, how it is communicated, and when it is communicated must conform to some mutually acceptable set of conventions between the entities involved. This set of conventions is referred to as a **protocol**, which may be defined as a set of rules governing the exchange of data between two entities [Ref. 16: p. 372].

1. Standard Versus Nonstandard Protocols

Standard or **open** protocols do not require a particular configuration in either hardware or software. Ideally, any vendor should be able to implement an open protocol on his machinery. To illustrate the concept of open protocols, consider a non-networking example--powering household appliances. In the United States, routine residential electrical power is available in homes by means of the standard two-prong electrical socket. Thousands of appliance manufacturers acknowledge this

standard, and develop cords and connectors that attach directly to this socket. Because of this standardization, consumers needn't be concerned about the buying the correct connector, or maintaining a supply of adapters. Both the user and vendor benefit from this arrangement, since they can focus on the function of the appliance rather than on the electrical connection.

By contrast, **nonstandard** or **proprietary** networking protocols are built for a specific networking situation, or particular model of computer [Ref. 16: p. 375]. Such protocols perform all functions satisfactorily in their specific situation, or on their specific computer type, but do not guarantee connectivity to other types of networks. As a non-networking example of a nonstandard protocol consider the formats used on video cassette tapes in the mid-1980's. There the Beta and VHS methods represented two totally functional, but totally dissimilar recording formats. The two formats had been developed independently by two manufacturers, without the benefit of predefined conventions. It took market forces years to establish a de-facto standard, VHS, but not before thousands of Beta video recorders were purchased by consumers.

2. Network Protocol Functions.

Protocols can be broad or narrow in scope. Some address a number of issues, others standardize just one aspect of a network's execution. In comprehensive

networking standards, the protocol will standardize the way that conforming nets execute each of the following functions:

- **Fragmentation**. Breaking data streams into standard-sized blocks;
- **Encapsulation**. Adding control information to data;
- **Connection Control**. Maintaining a connection between the source and destination;
- **Flow Control**. Limiting the amount of data the source sends while the destination is processing it;
- **Error Control**. Insuring data integrity;
- **Synchronization**. Establishing and maintaining mutual timing states between source and destination;
- **Sequencing**. Identifying the order in which data blocks are sent;
- **Addressing**. Establishing a unique addressing system for each entity on the network. [Ref. 16: pp. 376-383]

Standards-making bodies employ detailed scientific techniques to implement these functions; ones too complicated to describe here. However, it is important to appreciate the various network operations that these standards address.

B. INTERNETWORKING ALTERNATIVES: TCP/IP OR OSI

Both the TCP/IP and OSI protocol suites were mentioned the preceding chapters of this paper. And funding for both were included in the CNS Final Report. In this section, the suites will be discussed and their functions compared.

1. TCP/IP

TCP/IP is a set of protocols developed to allow cooperating, heterogeneous computers to share resources across a net. It was developed for use on the Defense Department's Advanced Research Project Agency Network (ARPANET), which remains part of the largest operational TCP/IP network. But with the growing need for internetworking in non-DOD networks, its use has spread greatly. By June, 1987, at least 130 vendors offered TCP/IP-based products. [Ref. 34: p. 1]

The terminology used in relation to these protocols can be very confusing. TCP and IP are actually two protocols out of a set of protocols. The most accurate name for this set is the **Internet Protocol Suite (IPS)**, since they are used on the Internet, a "network of networks," which includes ARPANET, MILNET, BITNET and 252 others participating networks [Ref. 35: p. 21]. Within the IPS, however, TCP and IP are the best known protocols, and the term, "TCP/IP," has come to stand for the whole suite. [Ref. 34: pp. 1-3] This convention has been followed throughout this paper, as it was in the text of the CNS Final Report.

a. The DOD-TCP/IP Link

Work on TCP/IP's oldest ancestors began in 1969 when scientists working at ARPA laboratories in California successfully got computers at four separate locations to

communicate with each other. DOD-funded research on the networking protocols continued until 1976 when a fully operational network, the forerunner of the DDN, was established. [Ref. 35: p. 21] In 1978, DOD endorsed versions of TCP/IP and mandated their use as DOD standards [Ref. 36: p. 109].

DOD's adoption of TCP/IP assured that implementations of the protocols would have a ready market. But the relationship with DOD furthered TCP/IP's acceptance in another significant way. DOD has maintained the DDN Network Information Center (NIC) which acts as a clearinghouse on TCP/IP-related issues.

The NIC provides general information and assistance to TCP/IP users, vendors and developers. It certifies vendor's TCP/IP compliance, and publishes the authoritative "TCP/IP Implementation and Vendors Guide," which is revised semi-annually and available for a nominal fee. The multi-volume "Official DDN Protocol Handbook" is also available to anyone interested. Finally, the NIC publishes, and maintains a library of, Requests for Comments or RFC's. These RFC's are documents soliciting responses from the Internet community on any DDN changes which have been proposed. RFC's have been used extensively to discuss modifications to the TCP/IP protocols. Thus the NIC has proved a valuable instrument in the proliferation of TCP/IP. [Ref. 37: pp. 49-52]

b. Functions of the TCP/IP Protocols

The TCP/IP family of protocols can be thought of as a box of tools that network users can employ when they need reliable communications with another network. [Ref: 34, p. 6]. Although the details of the protocols are complex, and are beyond the scope of this paper, the basic TCP/IP tools and their elementary functions are listed below, along with the RFC which describes their operation fully.

- **Simple Mail Transfer Protocol (SMTP)**: An effective electronic mail facility - RFC821 and RFC822;

- **Telnet**: Provides remote login to another computer - RFC854 and RFC855;

- **File Transfer Protocol (FTP)**: Supports file transfer between computers - RFC959;

- **Transmission Control Protocol (TCP)**: Breaks up messages into digestible segments, sends the segments, and re-assembles the message at the destination, with assurance against errors - RFC793;

- **Internet Protocol (IP)**: Finds the best route between source and destination for those message segments that TCP creates, and forwards them along the network - RFC791. [Ref. 34: pp. 6-11]

Many other services are available for use with the "basic" TCP/IP services listed above. They represent a superset of TCP/IP, and are frequently bundled as part of vendors' TCP/IP packages. For example, RFC989 describes privacy enhancements for internet mail, superceding SMTP. Remote execution (distinct from Telnet) is an option available to certain UNIX users. There are many other examples. In fact, a February, 1988, comparison of personal computer

TCP/IP implementations categorized 15 additional services which vendors were routinely offering [Ref. 38: pp. 1-3]. Although this proliferation of additional TCP/IP services can be confusing at times, its diversity is actually a credit to the flexibility and adaptability of the TCP/IP suite.

2. OSI Protocols

In 1977, the International Standards Organization chartered a subcommittee to develop common protocols to allow computer interoperability. Drawing upon the "lessons learned" when the ARPANET and certain European public communications networks were established, this ISO subcommittee developed and published the now-famous Open System Interconnection model in 1983. [Ref. 39: p. C/6] This model is based on the concept of seven vertical layers, each representing a networking function. Appendix D lists these seven layers and their functions. By partitioning the networking tasks in this manner, the OSI originators hoped to lend manageability to the discussion and development of complex network protocols. For comparison, Figure 5.1 is taken from Stallings [Ref. 16: p. 400] and contrasts the DOD Protocol Architecture with the OSI model.

Each layer in the model relies on the layer below it for services, just as it provides services to the layer above it. Communication should only occur between two adjacent layers; no layer should be bypassed. This layered

<table>
<tr><th>OSI</th><th>Internet Protocols</th></tr>
<tr><td>Application</td><td rowspan="3">Process/
Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Host-Host</td></tr>
<tr><td>Network</td><td>Internet</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network
Access</td></tr>
<tr><td>Physical</td></tr>
</table>

Figure 5.1 Comparison of ISO's OSI and the Internet Protocols

approach has gained much popularity since, "...it decomposes one (networking) problem into a number of manageable subproblems." [Ref. 16: p. 387]

Although the OSI reference model itself is not a protocol, ISO is responsible for certifying international protocols at layers 4 through 7 of its model. This has bred some confusing naming conventions. These "Layer 4 and above" ISO protocols are routinely referred to as "the OSI protocols," owing to the fact that the OSI model was central to their development. This naming convention, though not perfectly precise, will be followed in this paper.

Within this set of OSI protocols, the following have achieved the status of Draft International Standard: [Ref. 40: pp. 43-45]

OSI Layer	Service	Protocol Name
3	Internet	Internetwork Protocol (IP)
4	Transport	Transport Protocol-4 (TP-4)
7	E-Mail	CCITT X.400
7	E-Mail	ISO Message Handling System (MHS)
7	File Transfer	File Transfer and Access Management (FTAM)

Note the similarity in function to the TCP/IP, SMTP and FTP protocols. A standard to allow terminal access, the Virtual Terminal Protocol, is being developed but has not yet reached the status of draft standard [Ref. 40: p. 45]. As

was the case with TCP/IP, the OSI standards encompass a number of subordinate protocols providing the great utility to the network user.

3. TCP/IP and TP-4/IP Suites Compared

In a landmark 1985 paper, "Transport Protocols for Department of Defense Data Networks," the National Research Council summarized its evaluation of the two protocols by stating:

> A detailed comparison of the DOD Transmission Control Protocol and the ISO Transport Protocol indicates that they are **functionally equivalent** and provide essentially similar services. [Ref. 41: pp. 8-9]

The Council went on to say that although the transport layer protocols were similar, they were mutually incompatible, so network designers and users would have to choose between them. The Council therefore recommended that DOD transition to OSI because of their widespread use in Europe, where DOD required interoperability with NATO countries' computer networks. [Ref. 41: p. 11]

More recent evaluations indicate that although the transport and internetwork services of the two protocol suites are equivalent, TCP/IP does not compare well to the OSI protocols in two important areas: **security** and **network management**. [Ref. 42: p. 5]

a. Security

As they were originally configured, neither TCP/IP nor OSI fully satisfied government requirements for

highly secure data communications. However, the National Security Agency and the National Bureau of Standards (NBS) recently defined a security scheme for use on OSI-compliant networks called the Secure Data Network System (SDNS). SDNS employs encryption, authentication and access contrcl of user data to maintain confidentiality on networks. [Ref. 43: p. 1 and p. 84]

Development of systems such as the SDNS require a great deal of effort and expenditure of resources. For that reason it is unlikely that a TCP/IP-compatible variant of SDNS will be created. So security will likely remain a shortcoming of TCP/IP networks. This was described by Heiden, who in speaking of the Internet said, "Without encryption, we are all sending network postcards, available to almost anyone who wants to read them." [Ref. 35: p. 21]

b. Network Management

"Network management is probably the most notable flaw -- there really is no net management -- in TCP/IP (sic)," stated one networking technician at the 1987 Localnet East Exposition [quoted in Ref. 42: p. 5]. Although this technician is guilty of overstatement, TCP/IP net management reportedly does pale in comparison to the program under development by ISO.

The OSI Management Framework consists of four separate documents, each dealing with a different aspect of monitoring and controlling the activities on a network.

Each document is at a different stage of development. To date, the effort has taken seven years, and full adoption of these documents as international standards by 1990 is predicted. [Ref. 44: pp. 15-16]

4. OSI Availability

Although the OSI protocols listed in Paragraph 2, are still being fully defined, as of early 1988 all have been released by the ISO as Draft International Standards [Ref. 36: p. 109]. International vendors working primarily in Europe and Japan have used these draft documents to develop OSI-compliant products [Ref. 45: p. 2]. For a variety of reasons, US producers have not demonstrated as urgent a desire to implement the OSI standards in their products, despite announcements of support for the standards "in principle." [Ref. 46: pp. 41-42]

5. The Federal Government, DOD and OSI

The U.S. Government is the largest single buyer of networking products in the world. DOD is the largest single buyer of networking products in the U.S. Government. For that reason, U.S. and DOD policies toward the purchase of the OSI protocols greatly affect their marketability. Yet until July, 1987, a clear DOD strategy on incorporating the OSI protocols was difficult to determine from the guidance provided to DOD network managers and buyers since 1978.

The 1978 direction to make TCP/IP compulsory was very direct [Ref. 47: pp. 1-2]:

> To insure interoperability of future data networking, I am directing the adoption of a set of DOD standard host-to-host protocols based on TCP/IP. Use of these protocols is mandatory for packet-oriented networks.

But in 1982, DOD announced a preference for "commercial, off-the-shelf" products. TCP/IP was now considered a "government" protocol, in contrast to preferred "non-government" protocols, like the OSI suite. The Office of the Assistant Secretary of Defense for Information Resources (OSDIR) announced that DOD should:

> ... make every effort to inject DOD requirements into the non-government standard development through participation in standards forums. This influence should be exerted with the objectives of both avoiding the need to develop ... unique DOD standards and enabling eventual replacement of those unique standards with functionally equivalent non-government standards. [Ref. 48: pp. 1-2]

By 1985 the entire Federal Government was clearly moving toward OSI. The Government Open Systems Interconnection Procurement Specification (GOSIP), a major effort by government users and others to ease the transition to the OSI protocols, was under development by the National Bureau of Standards. GOSIP was to be the reference for all government agencies procuring ADP or communications systems and services.

In April, 1985, largely in response to the National Research Council's report discussed above (Paragraph B.3),

OSDIR announced DOD's strongest commitment to the international protocols:

> Whenever international standards are available and can be used to support military requirements, they will be implemented as rapidly as possible to obtain maximum economic and interoperability benefits. TP as a proven commercial offering is not available at this time. The progress of TP will be monitored carefully and once (it is) commercially available, TP will be tested for use in military applications. [Ref. 49: p. 2]

So certain DOD officials were tasked with monitoring the commercial progress of TP-4/IP, and wise network planners began making provisions for the inevitable transition to them.

However, by 1985 the business world had come to need the same type of interoperability that DOD had been enjoying since 1978. Since TCP/IP represented a mature, well-developed remedy for their networking problems, businesses and vendors flocked to the DOD protocols. It is ironic that while OSDIR was "carefully monitoring" the progress of TP-4, DOD's own TCP/IP protocols were hurting TP-4's commercial chances. As one business network analyst rhetorically asked:

> This resurgence of TCP/IP networks stymies the efforts of international standards bodies to implement OSI. With more TCP/IP products popping up, and users buying what's 'here and now', where does OSI fit in? [Ref. 50: p. 30]

Finally, in July 1987, an OSDIR memo outlined a long-term plan for DOD transition to OSI, tied directly to the outcome of the NBS GOSIP efforts. In this OSDIR document, the OSI protocols are designated as, "experimental

co-standards to the DOD protocols which provide similar service." They may be specified in addition to, in lieu of, or as an optional alternative to comparable DOD protocols. [Ref.51: p. 1.] Although that gives DOD agencies the opportunity to attempt an OSI-based network, the term "experimental" is meant to alert managers to the risks, both operational and economic, that they face in moving to the OSI protocols prematurely [Ref. 52: p. 13].

The July memo also reiterated DOD's support for the OSI protocols, once they have cleared the GOSIP conformance testing process. Although this GOSIP approval process may take months or even years, a clear timetable from point of approval forward is specified. The memo states:

> It is intended that DOD adopt the OSI protocols as a full co-standard with the DOD protocols when GOSIP is formally approved as a Federal Information Processing Standard. Two years thereafter, the OSI protocols would become the sole mandatory interoperable protocol suite. [Ref. 51: p. 1]

6. Implications for the NPS Campus Network

TCP/IP has reached maturity, and for the next few years, will probably remain the preferred protocols for communicating in a multivendor networking environment, both inside and outside of government. It has a solid manufacturer and customer base, and support for TCP/IP products will probably remain strong into the next decade. The TCP/IP suite provides services which are highly in

demand, and has enough flexibility to incorporate new applications as users demand them.

For these reasons, the choice of TCP/IP as the internetworking standards to be used initially on the Campus Network was astute. TCP/IP vendors offer products for virtually all of the LAN types identified in the BITS questionnaires, so product availability should not pose a problem. In addition, a number of NPS personnel have experience with TCP/IP from their work with the DDN. Their experience could prove a valuable resource when the Campus Network is brought on line.

On the other hand, most observers agree that it is just a matter of time before the OSI protocols claim the lion's share of the internetworking market. Their acceptance in Europe, Japan and other geographical areas will increase the urgency with which they are adopted here. Once substantial numbers of OSI-conforming products are approved by NBS, the DOD market will be opened, and the success of the protocols in the U.S. will be assured.

In the interim, however, there are simply not enough products available in the U.S. which conform to the OSI protocols. It was for that reason that the CNS decided on a phased migration to OSI. In this way TCP/IP will continue to provide network interconnectivity until the OSI products have been proven.

C. CHAPTER SUMMARY

This chapter began with a general look at the concept of networking protocols. Then the two prominent inter-networking protocol suites, TCP/IP and the OSI standards, were individually examined in terms of both their history and function. The two suites were then compared with each other, and their role in the government and DOD networking schemes discussed. Finally the strategy for choosing internetworking protocols for the NPS Campus Network was examined.

APPENDIX A

GLOSSARY

4B/5B. An encoding scheme used in the FDDI PHY specification.

ANSI. American National Standards Institute. A standards-making organization.

APD. Avalanche Photo Diode. An optical detector.

ARPANET. The Advanced Research Projects Administration Network, part of the DDN.

ASC X3T9.5. The ANSI Accredited Standards Committee which is working on the FDDI protocol specification.

Backbone Network. A transmission facility designed to interconnect lower-speed channels or terminals.

Bandwidth. The difference, expressed in cycles per second, between the highest and lowest frequencies of a band. It has also come to be equated with the data-carrying capability of a network.

Baseband. Transmission of signals without modulation. In a baseband LAN, digital signals are inserted directly onto the cable as voltage (electronic) or light (photonic) pulses. The entire spectrum of the cable is consumed by the signal.

BITS. The Base Information Transfer System.

Bridge. A device that links two homogeneous LAN's.

Broadband. A type of network which employs the modulation of a carrier frequency to carry many voice or data channels simultaneously.

CAD. Computer Aided Design.

CAI. Computer Aided Instruction.

CAM. Computer Aided Manufacturing.

CCIT. The International Telegraph and Telephone Consultative Committee. A standards-making organization under the United Nations and the International Telecommunications Union which recommends worldwide telecommunications standards.

Class A. Under FDDI a Class A station is one with direct connectivity to both of the network fiber cables.

Class B. Under FDDI a Class B station is one with direct connection to only one of the network fiber cables.

CSMA/CD. Carrier Sense Multiple Access with Collision Detection. A network access control method.

CNS. Connectivity and Networking Subcommittee of the NPS Mainframe Replacement Committee.

DDN. The Defense Data Network.

DEC. Digital Equipment Corporation of Maynard, MA.

DMDC. The Defense Manpower Data Center. An NPS tenant organization located in Monterey.

DOD. The Department of Defense.

DONIRM. Department of the Navy Information Resources Memorandum.

EMI. Electromagnetic interference.

EUC. End User Computing.

FDDI. Fiber Distributed Data Interface. Specifications under development by the ANSI for the standardization of high-speed fiber optic local area networks.

FNOC. Fleet Numerical Oceanography Center.

FOI. Fiber optic interface.

FTAM. The OSI File Transfer and Access Management Standard.

FTP. File Transfer Protocol.

Gateway. A network station or node which connects two dissimilar networks.

GBps. Gigabits per second. Billions of bits per second.

GOSIP. Government Open Systems Interconnection Procurement Specification.

IBM. International Business Machines Corporation of Armonk, New York.

IEEE. Institute of Electrical and Electronics Engineers. A standards-making organization.

IEEE 802.3. The IEEE specification for CSMA/CD (Ethernet) LAN's.

IEEE 802.5. The IEEE specification for token-passing ring LAN's.

IEEE 802.6. The IEEE specification for Metropolitan-Area (50 MBps) Networks.

IF. Interface. In this paper, it is the common boundary between two networks.

IP. Either the DOD Internet Protocol (TCP/IP); or the OSI Internetwork Protocol (TP-4/IP).

ISDN. Integrated Services Digital Network. A digital network allowing transmission of multiple information forms; often voice, data and video.

ISO. International Standards Organization.

KBps. Kilobits per second. Thousands of bits per second.

LAN. Local Area Network.

LASER. Light Amplification by Stimulated Emission of Radiation. Originally an acronym, now accepted as a standard term. A light energy source.

LED. Light-Emitting Diode. A light energy source.

LLC. Logical Link Control.

MAC. Medium Access Control. As it related to the FDDI, MAC refers to the functions specified in the Media Access Control document.

Manchester. A method of encoding data for transmission on a baseband network.

MBaud. Megabaud per second. Millions of baud per second.

MBps. Megabits per second. Millions of bits per second.

MENS. Mission Element Needs Statement.

MFM. Modified Frequency Modulation.

MHS. Message Handling System. One ISO electronic mail offering.

MHz. Millions of cycles per second.

MILNET. An unclassified military network, part of DDN.

NAVDAC. The Naval Data Automation Command.

NBS. The National Bureau of Standards.

NIC. The DDN Network Information Center.

Ohm. A measure of resistance in cable.

OSDIR. The Office of the Secretary of Defense for Information Resources.

OSI. ISO's Open System Interconnect seven layer model.

PHY. The FDDI Physical Layer Protocol.

PIN. A family of photo detector diodes.

PMD. The FDDI Physical Medium Dependent Protocol.

POC. In this context the BITS Point of Contact, or Project Officer for a given activity.

POM. Program Objectives Memorandum.

Proteon. Proteon Incorporated, of Westborough, MA.

RFC. Request for Comment.

SDNS. Secure Data Network System. An NBS security system for use with the OSI protocols.

SMT. The FDDI Station Management Protocol.

SMTP. Simple Mail Transfer Protocol. A DDN TCP/IP E-mail protocol.

TCP/IP. The Transmission Control Protocol/Internet Protocols. The DOD transport/internet layer protocols.

TP-4/IP. The Transport Protocol-4/Internetwork Protocols. The ISO transport/internet layer protocols.

TTR. FDDI´s Timed Token Rotation Protocol which guarantees minimum response time on the fiber ring.

VTP. The ISO Virtual Terminal Protocol.

APPENDIX B

BASE INFORMATION TRANSFER SYSTEM (BITS)
SURVEY QUESTIONNAIRE

BUILDING NO.________________

OFFICE or DEPARTMENT or ACTIVITY ________________

1. Respondant: Name ______________________________

Position ______________________________

Telephone ______________ Date ______________

2. How many people does the activity employ in this building? ______

3. How many of the activity's people in this building are primarily engaged in operating or maintaining a telecommunications system? Do not include those who operate computer systems unless the computers are used only to support telecommunications. ______

4. List the total numbers of the following systems/equipment items in this building used by the activity. Include acquisitions planned but not yet in hand; equipment types are defined in the glossary in Appendix C.

EQUIPMENT TYPE	EXISTING NUMBER	PLANNED NUMBER
a. Personal Computers	______	______
b. Terminals (tied to mainframe)	______	______
c. Graphics Terminals (primary function is graphics)	______	______
d. Word Processors	______	______
e. Hosts (generic name for mainframe)	______	______
f. Local Area Networks	______	______
g. Work Station	______	______

BUILDING NO.________________

5. Describe each local area network numbered in question 4. Enter the most valid "Topology", "Access", and "Media" according to the key below (see glossary in Appendix C for definitions). Enter the numbers of hosts and other devices connected to the system, and whether the system covers more than one building

NAME	PRIMARY MFGR	TOPOLOGY	ACCESS	MEDIA	NO. OF HOSTS	NO. OF DEVICES	MULTI-BLDG?

TOPOLOGY:

Star=S Bus=B
Ring=R Other=O

ACCESS SCHEME:

CSMA/CD=C
Token Passing=T
Other=O

MEDIA:

Twisted Pair=T Fiber=F
Baseband Coax=BA Other=O
Broadband Coax=BR

6. Describe any AISs or other telecommunications systems that the activity needs to access. If the primary manufacturer is unknown, leave blank. Check line type according to the key below. Enter the date the activity will start using the system; if already using, write "current". Enter "on" or "off" to indicate the location of the system host.

NAME	PRIMARY MANUFACTURER	LINE TYPE L	W	P	D	PLANNED ACCESS DATE	HOST ON OR OFF BASE?

LINE TYPES:
(See Glossary for defns)

L = LAN
P = Point-to-Point
(Point-to-point is a data circuit, not a local area network.)

W = WAN
D = Dial-up

BUILDING NO.________________

7. Check all levels of security required by the activity's current voice and data communications:

	TELEPHONE	DATA
Unclassified:	____	____
Confidential:	____	____
Secret:	____	____
Top Secret and Above:	____	____

8. At how many locations within the building will the activity need to originate a video broadcast? ____

For each location, enter the expected number of broadcasts per week, and briefly describe their purpose (training, video conferencing, etc.):

LOCATION (Room)	BROADCASTS PER WEEK	PURPOSE

9. How many telephones does the activity have in this building? ____

10. Check all of the types of telephone instruments used:

Key ___ Rotary ___ TouchTone (tm) ___

Security Terminal Unit (STU) I ___ STU II ___ STU III ___

Integrated Voice/Data Set (e.g. DisplayPhone) ___

PAGE 3 of 6

BUILDING NO.________

11. Enter the maximum number of separate, simultaneous conference calls the activity needs to establish in the building: ____

12. Enter the maximum number of participants the activity normally needs to include in a conference call: ____

13. Estimate the number of the activity's staff in this building that place and receive the following numbers of phone calls per day:

    Less than 10 ______ 10 or more ______

14. Estimate the number of the activity's calls in this building that are made to or received from per day:

    On Base ______ Off Base (Local) ______

    FTS/Autovon ______ Commercial Long Distance ______

15. Does the activity *maintain* a Defense Data Network (DDN) node in the building? (Answer "yes" only if you have the node itsef.) Yes ___ No ___

16. If the activity controls the building, check the physical security requirements it has and those it needs: (Consider the "need" column to be a wish list. If you want it, put it down.)

	HAVE:	NEED:
Access control into building? (card systems, telephone access)	____	____
Electronic barriers at entrances? (elevator control, parking systems)	____	____
Personal Identification at entrances? (Id badges, finger print systems)	____	____
Intrusion detection into building? (door sensors, motion detectors, alarms)	____	____
CCTV system inside of building? (cameras, monitors, controls)	____	____

BUILDING NO.________________

17. Does the activity need a public address system within the building:

Yes: ____ No: ____

18. Please describe the activity's programmed budget (in terms of amounts POM'd) to support staff in this building for the following purposes: already approved.

Fiscal Year:	FY90	FY91	FY92	FY93	FY94
OPS OLD (Operations/maintenance for existing telecom. systems; include LANs, AISs; if possible, exclude single-building systems)					
OPS NEW (Operations/maintenance for planned systems)					
OPS SECRTY (Operations/maintenance for planned security equipment)					
PUR NEW (Purchase costs for planned systems)					
PUR SECRTY (Purchase costs for security equipment)					

BUILDING NO.________________

19. Describe any specific improvements in current voice or data communications requested by activity staff in this building (including pier operations, if applicable):

20. List additional communications requirements (e.g., laser, microwave, satellite communications, encryption devices, etc.) (This is another wish list. If you want it, put it down.)

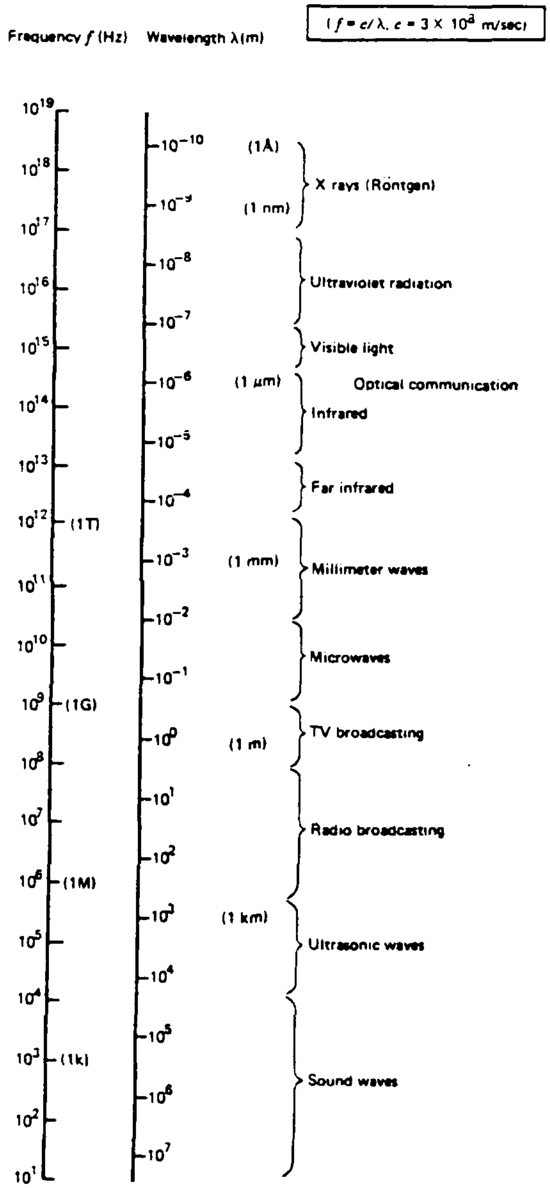
21. **Additional Comments:** (List any particular requirements you have have such as the need to communicate with another base or installation. This is another wish list. Go for broke. List anything you want.)

PAGE 6 of 6

APPENDIX C

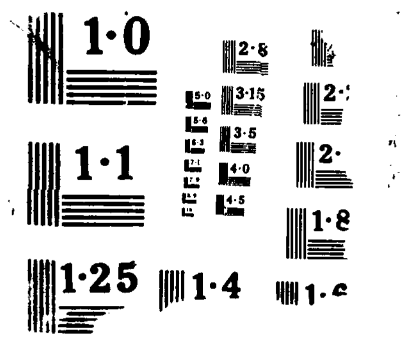
Frequency and Spectrum Chart

Conversion Between Frequency f and Wavelength λ



AD-A195 444 THE PROPOSED NAVAL POSTGRADUATE SCHOOL CAMPUS NETWORK: COMPUTER COMMUNICATIONS FOR THE 1990'S(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA K M LEAHY MAR 88 2/2

UNCLASSIFIED F/G 12/7 NL


1·0
2·8
3·15
3·5
4·0
4·5
1·1
1·8
1·25
1·4

APPENDIX D

The Open System Interconnect Layers

1.	**Physical**	Concerned with the transmission of unstructured bit streams over the physical medium. Deals with the mechanical, electrical functional and procedural characteristics to access the physical medium;
2.	**Data Link**	Provides for the reliable transfer of information across the physical link;
3.	**Network**	Responsible for establishing, maintaining and terminating connections;
4.	**Transport**	Provides for reliable, transparent transfer between end points; provides end-to-end error recovery and flow control;
5.	**Session**	Provides control structures to communicate between applications, establishes sessions between sessions;
6.	**Presentation**	Provides independence to the application processes from differences in data representation (syntax);
7.	**Application**	Provides access to the OSI environment for users and also provides distributed information services.

LIST OF REFERENCES

1. Connectivity and Network Committee of the NPS Mainframe Computer Replacement Committee, Connectivity and Network Report: Campus Computer Network, Naval Postgraduate School, 15 November 1987.

2. Connectivity and Network Committee, Minutes of Committee Meeting, Naval Postgraduate School, September 1987.

3. Connectivity and Network Committee, Minutes of Committee Meeting, Naval Postgraduate School, 11 September 1987.

4. Schneidewind, Norman F., "Principles of Local Area Networks," Encyclopedia of Science and Technology, McGraw-Hill Publishers, 1986.

5. Connectivity and Network Committee, Minutes of Committee Meeting, Naval Postgraduate School, 9 October 1987.

6. Connectivity and Network Committee, Minutes of Committee Meeting, Naval Postgraduate School, 23 October 1987.

7. Connectivity and Network Committee, Minutes of Committee Meeting, Naval Postgraduate School, 30 October 1987.

8. Huber, N., Data Communications Terms, Datacomm Group Publishers, 1986.

9. Department of the Navy, Office of Information Resource Management, DONIRM No. 107, Subject: Local Area Network (LAN) Planning, 15 November 1985.

10. Department of the Navy, Office of Information Resources Management, DONIRM No. 71, Subject: Data Communications Planning, 30 July 1986.

11. Naval Data Automation Command, Base Information Transfer System (BITS) User Survey Guidelines, 1 May 1986.

12. Department of the Navy, Office of Information Resources Management, DONIRM No. 155, Subject: Data Communications Planning, 18 December 1986.

13. Naval Postgraduate School Letter 5230 over NC4(44) to Distribution List 1, Subject: BASE INFORMATION TRANSFER SYSTEM (BITS) SURVEY, 28 September 1987.

14. Naval Postgraduate School Computer Center Memorandum From: Ms. A. L. Austin and Ms. C. J. Miller, To: LCDR M. E. Anderson, Subject: BITS Survey, 17 December 1987.

15. Office of the Assistant Secretary of Defense for Command, Control and Communications Memorandum to Secretaries of the Military Departments and the Chairman, Joint Chiefs of Staff, Subj: Open Systems Interconnection Protocols, 2 July 1987.

16. Stallings, W., Data and Computer Communications, Macmillan Publishing Company, 1985.

17. Herman, J., "Orders of Magnitude," in Network World, Volume 4, Number 24, p. 27, 15 June 1987.

18. Suematsu, Y., and Iga, K., Introduction to Optical Fiber Communications, Wiley and Sons Publishers, 1982.

19. Sandbank, C. P., (editor), Optical Fibre Communication Systems, Wiley and Sons Publishers, 1980.

20. CommunicationsWeek, "AT&T Gigabit System Links Two COs," Volume 164, p. 36, 5 October 1987.

21. Derfler, F., "Optical Communications: A Technical Primer," PC Magazine, Volume 7, Number 1, p. 262, 12 January 1988.

22. Bubbeo, D., "Wire, Cable Manufacturers Bow At Last to Pressure to Raise Prices," Electronic Buyers' News, p. T6, 10 August 1987.

23. Burr, W. E., "The FDDI Optical Data Link," IEEE Communications Magazine, Volume 24, Number 5, p. 21, May 1986.

24. CommunicationsWeek, "Bellcore Achieves New Fiber Optic Transmission Speed," Volume 171, p. 65, 23 November 1987.

25. Barnoski, M. K., "Fiber Systems for the Military Environment," Proceedings of the IEEE, Volume 68, Number 10, p. 1315, October 1980.

26. Joshi, S., "High Performance Networks: A Focus on the Fiber Distributed Data Interface Standard," IEEE Micro, Volume 6, Number 3, p. 8, June 1986.

27. Ross, F. E, "FDDI -- A Tutorial," IEEE Communications Magazine, Volume 24, Number 5, p. 10, May 1986.

28. Ullal, J., "FDDI Network Facilitates Data Faster Than a Speeding Bullet," Computer Technology Review, Volume VII, Number 14, p. 38, November 1987.

29. Green, L., "Planning For FDDI," Proceedings of the IEEE 12th Conference on Local Computer Networks, p. 4, October, 1987.

30. Salwen, H., "How to Get Ready for FDDI Challenges and Opportunities," Proceedings of the IEEE 12th Conference on Local Computer Networks, p. 12, October, 1987.

31. Musich, P., "FDDI Standard Advances With Fibronics Device," Network World, Volume 4, Number 47, p. 15, 23 November 1987.

32. Kolnik, I., and Garodnick, J., "First FDDI Local Area Network," Proceedings of the IEEE 12th Conference on Local Computer Networks, p. 7, October 1987.

33. Miller, A. R., "1986: The Year of Networking," IEEE MICRO, Volume 6, Number 3, p. 6, June 1986.

34. Hedrick, C. L., Introduction to the Internet Protocols, Rutgers University, 1987.

35. Miles, J.B., "'The Father of DDN' Discusses Internet," Government Computer News, p. 21, 31 July 1987.

36. Rehki, K., "Transparent Access to Mixed Equipment Leads From TCP/IP to OSI," Computer Technology Review, Volume VII, Number 16, pp. 109-113, Winter 1987.

37. Defense Communications Agency, DDN New User Guide, Dennett, S. C., and others, pp. 49-52, December, 1985.

38. Nussbacher, H., "PC/IP Scorecard," PC/IP Forum, Internet Message <8802220249.aa24157@Louie.UDEL.EDU>, February, 1988.

39. Pompili, A., "Government Taking Reins in OSI," PC WEEK, Volume 1, Number 37, pp. C/6-C/8, 15 September 1987.

40. National Bureau of Standards, U.S. Open System Interconnection User's Committee, "Government Open Systems Interconnection Procurement Specification for Years 1987 and 1988 (Draft)," March 1987.

41. National Research Council of the National Academy of Sciences, Transport Protocols for the Department of Defense Data Networks, pp. 2-10, National Academy Press, February, 1985.

42. Musich, P., "Vendors See TCP/IP as ISO Standards Stopgap," Network World, Volume 4, Number 25, p. 5, 22 June 1987.

43. DePompa, B., "Parties Agree on 'Secure' OSI," CommunicationsWeek, Volume 163, p. 1, 28 September 1987.

44. Petrosky, M., "Management Standard Near," Network World, Volume 4, Number 26, pp. 15-16, 29 June 1987.

45. Rose, M., and Cass, D., "ISO Transport Services on Top of the TCP: Version 3," Request for Comment 1006, p. 2, May, 1987.

46. Powers, P., and Moore, S., "Who's Most Open of Them All?," Network World, Volume 4, Number 49, pp. 41-44, 7 December 1987.

47. Office of the Secretary of Defense for Information Resources, "Host-to-Host Protocols for Data Communications Networks," pp. 1-2, December, 1978.

48. Office of the Secretary of Defense for Information Resources, "DOD Policy on Standardization of Host-to-Host Protocols," p. 3, March, 1982.

49. Office of the Secretary of Defense for Information Resources, "National Research Council Report on Transport Protocols for DOD Data Networks," pp. 1-3, April, 1985.

50. Bride, L., quoted in Jackson, K., "Government Still Talks TCP/IP While Waiting Word on GOSIP," CommunicationsWeek, Volume 173, p. 30, 7 December 1987.

51. Office of the Secretary of Defense for Information Resources, "Open System Interconnection Protocols," pp. 1-3, 2 July 1987.

52. Latham, D., "DOD Should Stay the Course on Ada," Federal Computer Week, Volume 1, No. 23, p. 13, 7 September 1987.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, CA 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Director of Information Systems Officer of Chief of Naval Operations (OP-0945) Navy Department Washington, D. C. 20350-2000	1
4.	Department Chairman, Code 54 Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
5.	Curricular Officer, Code 37 Naval Postgraduate School Monterey, CA 93940-5000	2
6.	Superintendent Attn: Prof. N. F. Schneidewind, Code 54Ss Naval Postgraduate School Monterey, CA 93940-5000	1
7.	Superintendent Attn: Y. K. Mortagy, Code 54My Naval Postgraduate School Monterey, CA 93940-5000	1
8.	Commanding Officer Attn: Capt. K. M. Leahy, USMC Marine Corps Tactical Systems Support Activity Camp Pendleton, CA 92055-5000	4

END
DATED
FILM
8-88
DTIC